

OCT 28 2019

UNITED STATES DISTRICT COURT

AT SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
BY DEPUTY

for the

Western District of Washington

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Sixteen (16) Subject Devices described in Attachment A
stored in the Federal Bureau of Investigation, Seattle Field
Office, located at 1110 3rd Ave., Seattle, WA 98101

Case No.

MJ19-515

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, incorporated herein by reference.

located in the WESTERN District of WASHINGTON, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

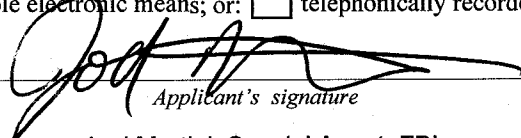
Code Section	Offense Description
18 U.S.C. §§ 2252(a)(2) & 2252(a)(4)(B)	Receipt or Distribution of Child Pornography and Possession of Child Pornography

The application is based on these facts:

- ☒ See Affidavit of Joel Martini, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☐ by reliable electronic means; or: ☐ telephonically recorded.

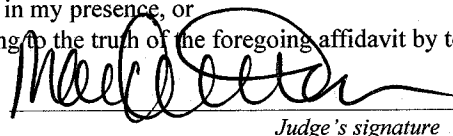

Applicant's signature

Joel Martini, Special Agent, FBI

Printed name and title

- ☒ The foregoing affidavit was sworn to before me and signed in my presence, or
☐ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 10/28/2019


Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge

Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) ss
 COUNTY OF KING)

I, Joel Martini, being duly sworn, declare and state as follows:

INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation (FBI), currently assigned to the Seattle Field Office, and have been so employed since January 2017. I am assigned to the Cyber squad where I primarily investigate computer intrusions and other Cybercrimes. My experience as an FBI Agent includes the investigation of cases involving the use of computers and the Internet to commit crimes. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, Cybercrimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. I have personally participated in the execution of search warrants involving the search and seizure of computer equipment. I have received advanced training in the acquisition and analysis of digital evidence (both network and host based), responding to computer intrusions and other incidents. I currently hold a Bachelor's of Science in Information Systems from Corban University.

2. Prior to my employment as a Special Agent, I worked as a Computer Forensic Examiner for the FBI for approximately 5 years. As part of that employment, I became familiar with the design and operations of various electronic devices, networks, and websites, including technology described herein. I also became familiar with criminal violations relating to child exploitation and child pornography including violations of Title 18, United States Code § 2252.

PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the following devices, including a mirror image thereof, all of which are currently located at the Federal Bureau of Investigation, Seattle Field Office, at 1110 3rd Ave, Seattle, WA 98101, and were initially seized on about June 19, 2019, from 40520 Aster Place, Palmdale, California:

Item Description	FBI Evidence Number
1. One (1) HGST hard drive, S/N: 130325TEA45A3R240BK;	1B2
2. One (1) HGST hard drive, S/N: 130301E20342BM0V340S;	1B3
3. One (1) Hitachi hard drive, S/N: 111223E20B12C7CGL9RS;	1B4
4. One (1) Toshiba hard drive w/ power cord, G003250A;	1B5
5. One (1) Seagate hard drive w/enclosure, S/N: Z84112WS, S/N: NA8TLMTO;	1B8
6. Two (2) 4GB Powersticks, Model PSPV1;	1B10
7. One (1) Kodak memory card 8GB w/case, 31295-8GBCSTA;	1B14
8. One (1) ETC hotels thumb drive, 1GB 1011S;	1B15
9. One (1) ETC hotels thumb drive, 1GB 1011S;	1B16
10. One (1) Casa del Mar ETC hotel flashdrive 2GB;	1B17
11. One (1) Transcend Micro SD adapter 32GB, 9181AA32G09QS2;	1B18
12. One (1) Kingston Technologies hard drive 128GB, 50026B7726A02E6DE;	1B21
13. One (1) iPhone S, rose gold color, Model: A1633;	1B25
14. One (1) iPhone, black, Model: A1778;	1B28
15. One (1) Macbook w/power cord, S/N: C02MN8TDFD57;	1B32
16. One (1) iPhone X, black, cracked back	1B33

("SUBJECT DEVICES"), as described in Attachment A, for the items to be seized described in Attachment B, which are incorporated herein by reference.

4. The warrant would authorize a search of the SUBJECT DEVICES and forensic examination of their content, for the purpose of identifying electronically stored data as particularly described in Attachment B, for evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography)

6. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

The following definitions apply to this Affidavit:

7. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

8. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the

1 visual depiction has been created, adapted, or modified to appear that an identifiable
2 minor is engaged in sexually explicit conduct.

3 9. "Computer," as used herein, refers to "an electronic, magnetic, optical,
4 electrochemical, or other high speed data processing device performing logical or storage
5 functions, and includes any data storage facility or communications facility directly
6 related to or operating in conjunction with such device" and includes smartphones, and
7 mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

8 10. "Computer hardware," as used herein, consists of all equipment that can
9 receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit
10 electronic, magnetic, or similar computer impulses or data. Computer hardware includes
11 any data-processing devices (including central processing units, internal and peripheral
12 storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes,
13 and other memory storage devices); peripheral input/output devices (including keyboards,
14 printers, video display monitors, and related communications devices such as cables and
15 connections); as well as any devices, mechanisms, or parts that can be used to restrict
16 access to computer hardware (including physical keys and locks).

17 11. "Computer passwords and data security devices," as used herein, consist of
18 information or items designed to restrict access to or hide computer software,
19 documentation, or data. Data security devices may consist of hardware, software, or
20 other programming code. A password (a string of alphanumeric characters) usually
21 operates what might be termed a digital key to "unlock" particular data security devices.
22 Data security hardware may include encryption devices, chips, and circuit boards. Data
23 security software may include programming code that creates "test" keys or "hot" keys,
24 which perform certain pre-set security functions when touched. Data security software or
25 code may also encrypt, compress, hide, or "booby-trap" protected data to make it
26 inaccessible or unusable, as well as reverse the process to restore it.

27 12. Internet Service Providers (ISPs), as used herein, are commercial
28 organizations that are in business to provide individuals and businesses access to the

1 internet. ISPs provide a range of functions for their customers including access to the
2 Internet, web hosting, email, remote storage, and co-location of computers and other
3 communications equipment. ISPs can offer a range of options in providing access to the
4 Internet including telephone based dial up, broadband based access via digital subscriber
5 line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs
6 typically charge a fee based upon the type of connection and volume of data, called
7 bandwidth, which the connection supports. Many ISPs assign each subscriber an account
8 name – a user name or screen name, an “email address,” an email mailbox, and a
9 personal password selected by the subscriber. By using a computer equipped with a
10 modem, the subscriber can establish communication with an ISP over a telephone line,
11 through a cable system or via satellite, and can access the Internet by using his or her
12 account name and personal password. ISPs maintain records pertaining to their
13 subscribers (regardless of whether those subscribers are individuals or entities). These
14 records may include account application information, subscriber and billing information,
15 account access information (often times in the form of log files), email communications,
16 information concerning content uploaded and/or stored on or via the ISP's servers.

17 13. “Internet Protocol address” or “IP address” refers to a unique number used
18 by a computer to access the Internet. An IP address often looks like a series of four
19 numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every
20 computer connected to the Internet must be assigned an IP address so that the Internet
21 traffic sent from, and directed to, that computer may be properly directed from its source
22 to its destination. Most ISPs control the range of IP addresses.

23 14. The “Internet” is a global network of computers and other electronic
24 devices that communicate with each other. Due to the structure of the Internet,
25 connections between devices on the Internet often cross state and international borders,
26 even when the devices communicating with each other are in the same state.

27 15. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the
28 age of eighteen years.

1 16. “Records,” “documents,” and “materials,” as used herein, include all
2 information recorded in any form, visual or aural, and by any means, whether in
3 handmade, photographic, mechanical, electrical, electronic, or magnetic form.

4 17. “Remote Computing Service” (“RCS”), as defined in 18 U.S.C. § 2711(2),
5 is the provision to the public of computer storage or processing services by means of an
6 electronic communications system.

7 18. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means
8 actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-
9 genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality;
10 (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the
11 genitals or pubic area of any person.

12 19. A “storage medium” is any physical object upon which computer data can
13 be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-
14 ROMs, and other magnetic or optical media.

15 20. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes
16 undeveloped film and videotape, data stored on computer disc or other electronic means
17 which is capable of conversion into a visual image, and data which is capable of
18 conversion into a visual image that has been transmitted by any means, whether or not
19 stored in a permanent format.

20 **SUMMARY OF PROBABLE CAUSE**

21 21. As set forth in Exhibit 1, the FBI Seattle Office is conducting an
22 investigation into a data breach and network intrusions of Nintendo, a consumer
23 electronics and video game company. Nintendo of America is located in Redmond,
24 Washington. The parent company, Nintendo Co., Ltd, is headquartered in Japan.
25 Nintendo has manufactured a variety of home and handheld game consoles, such as the
26 Wii U, 3DS, and the Switch, and developed multiple popular video game franchises, such
27 as Mario, The Legend of Zelda, Pokémon, Animal Crossing, and Splatoon, among others.
28

1 22. As set forth in Exhibit 1, the FBI identified the suspected hacker as RYAN
2 HERNANDEZ, also known as "Ryan West" and "RyanRocks" ("HERNANDEZ"), an
3 individual previously known to the FBI and to Nintendo for prior hacking conduct
4 targeting Nintendo and its products. At all relevant times, HERNANDEZ resided at
5 40520 Aster Place, Palmdale, California 93551 (SUBJECT PREMISES).

6 23. As set forth in Exhibit 1, FBI agents, including myself, interviewed
7 HERNANDEZ in October 2017 at the SUBJECT PREMISES regarding a prior hack of
8 Nintendo's Developer Portal and the dissemination of stolen proprietary data. Despite
9 HERNANDEZ's promises to cease such activity, he subsequently conducted an even
10 larger compromise and intrusion of various Nintendo networks.

11 24. As set forth in Exhibit 1, HERNANDEZ was identified through various
12 methods, including use of IP addresses associated with the SUBJECT PREMISES.
13 HERNANDEZ also openly discussed hacking activity and specifically his theft of
14 Nintendo data on various online forums, including Discord and Twitter.

15 25. On June 18, 2019, I obtained a federal search warrant issued by the
16 Honorable Maria A. Audero, United States Magistrate Judge, in the Central District of
17 California, authorizing the search of the SUBJECT PREMISES. The warrant, which is
18 incorporated herein by reference, authorized the seizure of digital devices from the
19 SUBJECT PREMISES for a period of 120 days to allow the government to search such
20 devices for evidence of violations of Title 18, United States Code, Sections 371 and 1349
21 (Conspiracy), 1028(a)(7) (Identity Theft); 1028A (Aggravated Identity Theft); 1029(a)(2)
22 (Access Device Fraud); 1030(a)(2), (4) and (5)(A) (Computer Fraud/Hacking); and 1343
23 (Wire Fraud).¹

24 26. On June 19, 2019, federal agents, including myself, and other assisting law
25 enforcement officers executed the warrant at the SUBJECT PREMISES. HERNANDEZ
26
27

28 ¹ As further set forth in Exhibit 1, the court authorized an extension of the 120-period for the retention and examination of the seized devices for an additional 120 days, to February 13, 2020.

was present, as were his parents. Specifically, HERNANDEZ was inside his bedroom when agents initially arrived.

27. During the search of the SUBJECT PREMISES, federal agents located and seized the following 32 digital devices, which includes the SUBJECT DEVICES:

Item Description	FBI Evidence Number
1. One (1) HGST hard drive, S/N: 130325TEA45A3R240BK;	1B2
2. One (1) HGST hard drive, S/N: 130301E20342BM0V340S;	1B3
3. One (1) Hitachi hard drive, S/N: 111223E20B12C7CGL9RS;	1B4
4. One (1) Toshiba hard drive w/ power cord, G003250A;	1B5
5. One (1) Nintendo Switch w/power cord, XAW10001300634;	1B6
6. One (1) Nintendo Switch w/power cord, XAL03100140300;	1B7
7. One (1) Seagate hard drive w/enclosure, S/N: Z84112WS, S/N: NA8TLMT0;	1B8
8. One (1) Wii w/power cord, S/N: RMA200086644;	1B9
9. Two (2) 4GB Powersticks, Model PSPV1;	1B10
10. One (1) Apple Watch, FH7QM3CBGR7N;	1B11
11. One (1) adapter, E202650;	1B12
12. One (1) Motorola Micro SD adapter, 2010-06-12;	1B13
13. One (1) Kodak memory card 8GB w/case, 31295-8GBCSTA;	1B14
14. One (1) ETC hotels thumb drive, 1GB 1011S;	1B15
15. One (1) ETC hotels thumb drive, 1GB 1011S;	1B16
16. One (1) Casa del Mar ETC hotel flashdrive 2GB;	1B17
17. One (1) Transcend Micro SD adapter 32GB, 9181AA32G09QS2;	1B18
18. Four (4) CDs;	1B19
19. One (1) Nintendo 3DS w/adapter, EW100000054	1B20
20. One (1) Kingston Technologies hard drive 128GB, 50026B7726A02E6DE;	1B21
21. One (1) Nintendo WiiU, JW403398933;	1B22
22. One (1) IS-Nitro-Emulator, S/N: 08050639;	1B23
23. One (1) WiiU, FW705088709;	1B24
24. One (1) iPhone S, rose gold color, Model: A1633;	1B25
25. One (1) Nintendo Switch w/cradle and power cord, XAW10021377616;	1B26
26. One (1) blue Nintendo 3DSXL, SW105787592;	1B27
27. One (1) iPhone, black, Model: A1778;	1B28
28. One (1) Nintendo WiiU black, FW99906933;	1B29
29. One (1) NDEV wireless w/power cord, S/N: NMA20089065;	1B30
30. One (1) WiiU, white w/controller S/N: FW090204951;	1B31
31. One (1) Macbook w/power cord, S/N: C02MN8TDFD57;	1B32

32. One (1) iPhone X, black, cracked back	1B33
---	------

28. All above listed devices were recovered from HERNANDEZ's bedroom within the SUBJECT PREMISES. Among these items was an 8TB Seagate hard drive, S/N: Z84112WS, S/N: NA8TLMT0 (FBI Evidence No. 1B8), that was located in a plastic crate in HERNANDEZ's bedroom, underneath the bed.

29. After the search of the SUBJECT PREMISES, the Seagate hard drive and other digital devices, including the SUBJECT DEVICES, were packaged, logged into evidence control, and transferred from FBI Los Angeles to FBI Seattle for analysis and examination pursuant to the ongoing investigation.

30. On October 16, 2019, I was advised by FBI Seattle's computer forensic examiners that the Seagate hard drive in particular was ready for analysis and review.

31. On October 22, 2019, while looking at files located on the Seagate hard drive pursuant to the above-referenced search warrant, I observed numerous files that, based on my training and experience and my involvement in this investigation, I recognized as stolen Nintendo files and data.

32. During my review, I accessed a folder named "BAD STUFF" that contained multiple subfolders, including one named "cute." Inside of the "cute" subfolder, I observed approximately 336 video and graphics files that, based on my training and experience, appeared to be consistent with child pornography. For instance, numerous filenames were overtly sexually suggestive and referenced minors and juvenile age ranges. While employed with FBI, I have examined numerous devices containing child pornography and have worked on, and am familiar with, child exploitation and child pornography investigations.

33. Specifically, within the "cute" subfolder, I observed the presence of the following files, which I reviewed and describe below:

- BR160 12 and 7 Year Old Cousins Suck Fuck 69 And Jerk + Get Caught.avi

- This 50-minute video depicts two prepubescent males on a webcam sitting on what appears to be a bed. Both males remove their clothing and proceed to engage in both manual and oral sex. Based on lack of pubic hair, muscular development, and youthful appearance, I estimate that both males are approximately between 7 and 12 years old (as indicated by the file name).
- 2 boys hard fuck xxx.avi
 - This 20-minute video depicts a naked prepubescent male laying on a bed. A second prepubescent male is shown removing his clothing and joining the first male on the bed. The video continues to show the pair engaging in oral and anal sex. Based on lack of pubic hair, muscular development, and youthful appearance, I estimate that both males are approximately 12 years old.
- 9 Year Old Zachary And Kevin Suck Jerk And Play + Get Caught.avi
 - This 58-minute video depicts two prepubescent males on a webcam sitting on what appears to be a bed. Both males remove their clothing and proceed to engage in both manual and oral sex. Based on lack of pubic hair, muscular development, and youthful appearance, I estimate that both males are approximately 9 years old (as indicated by the file name).

I believe each of these files to depict minors engaging in sexually explicit conduct.

Based on the filename and the circumstances, I further believe that the other video and graphic files in the “cute” subfolder depicted similar conduct involving minors.

34. Immediately after observing examples of what I recognize to be child pornography, I ceased review of the digital evidence and contacted the United States Attorney’s Office. I have only accessed the plain-view possible child pornography files to gather details for this affidavit. FBI has halted its review pending an application for a supplemental search warrant authorizing the search and seizure of child pornography and related material, as described in Attachment B.²

² The United States Attorney’s Office for the Central District of California (“CDCA”) was also alerted to the discovery of suspected child pornography and the FBI’s desire to obtain a supplemental search warrant. CDCA
 Affidavit of Special Agent Joel Martini – 10
 USAO# 2018R01269

UNITED STATES ATTORNEY
 700 STEWART STREET, SUITE 5220
 SEATTLE, WASHINGTON 98101
 (206) 553-7970

35. On October 23, 2019, FBI Special Agent Benjamin Williamson and Special Agent Ian Burns viewed the three video files described above. SA Williamson and SA Burns are both assigned to FBI Seattle's Child Exploitation Task Force and have received advanced training on child pornography and related investigations. Both SA Williamson and SA Burns concurred with the descriptions above and opined that the files depicted minors engaging in sexually explicit conduct.

36. Based on my training and experience and the information relayed to me by other law enforcement officers with experience investigating the sexual exploitation of children, I believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), is likely to be found on the SUBJECT DEVICES.

TECHNICAL BACKGROUND

39. As part of my training, I have become familiar with the Internet, a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high speed telecommunications links (e.g., copper and fiber optic cable), and wireless transmissions, including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via email.

40. Based on my training and experience, I know that cellular phones (referred to herein generally as "smart phones") have the capability to access the Internet and store information, such as videos and images. As a result, an individual using a smart phone

agreed that, because the devices and images thereof, were currently located in Seattle, and in conjunction with a FBI Seattle investigation, that the supplemental search warrant should be properly sought in the Western District of Washington.

1 can send, receive, and store files, including child pornography, without accessing a
2 personal computer or laptop. An individual using a smart phone can also easily plug the
3 device into a computer, via a USB cable, and transfer data files from one digital device to
4 another. People generally carry their smart phone on their person; recent investigations
5 in this District have resulted in the discovery of child pornography files on smart phones
6 which were carried on an individual's person at the time the phones were seized.

7 41. As set forth above and in Attachment B to this Affidavit, I seek permission
8 to further search for and seize evidence, fruits, and instrumentalities of the above-
9 referenced crimes that might be on the SUBJECT DEVICES, in whatever form they are
10 found. It has been my experience that individuals involved in child pornography often
11 prefer to store images of child pornography in electronic form. The ability to store
12 images of child pornography in electronic form makes digital devices, examples of which
13 are enumerated in Attachment B to this Affidavit, an ideal repository for child
14 pornography because the images can be easily sent or received over the Internet. As a
15 result, one form in which these items may be found is as electronic evidence stored on a
16 digital device.

- 17 a. Based upon my knowledge, training, and experience in child
18 exploitation and child pornography investigations, and the
19 experience and training of other law enforcement officers with
20 whom I have had discussions, I know that computers and computer
21 technology have revolutionized the way in which child pornography
22 is collected, distributed, and produced. Through the use of
23 computers and the Internet, distributors of child pornography use
24 membership based/subscription based websites to conduct business,
25 allowing them to remain relatively anonymous.
- 26 b. In addition, based upon my own knowledge, training, and experience
27 in child exploitation and child pornography investigations, and the
28 experience and training of other law enforcement officers with
whom I have had discussions, I know that the development of
computers has also changed the way in which those who seek out
child pornography are able to obtain this material. Computers serve
four basic functions in connection with child pornography:

1 production, communication, distribution, and storage. More
2 specifically, the development of computers has changed the methods
3 used by those who seek to obtain access to child pornography as
4 described in subparagraphs (c) through (f) below.

5 c. Producers of child pornography can now produce both still and
6 moving images directly from the average video or digital camera.
7 These still and/or moving images are then uploaded from the camera
8 to the computer, either by attaching the camera to the computer
9 through a USB cable or similar device, or by ejecting the camera
10 memory card from the camera and inserting it into a card reader.
11 Once uploaded to the computer, the images can then be stored,
12 manipulated, transferred, or printed directly from the computer.
13 Images can be edited in ways similar to those by which a photograph
14 may be altered. Images can be lightened, darkened, cropped, or
15 otherwise manipulated. Producers of child pornography can also use
16 a scanner to transfer printed photographs into a computer-readable
17 format. As a result of this technology, it is relatively inexpensive and
18 technically easy to produce, store, and distribute child pornography.
19 In addition, there is an added benefit to the pornographer in that this
20 method of production does not leave as large a trail for law
21 enforcement to follow.

22 d. The Internet allows any computer to connect to another computer.
23 By connecting to a host computer, electronic contact can be made to
24 literally millions of computers around the world. A host computer is
25 one that is attached to a network and serves many users. Host
26 computers, including ISPs, allow email service between subscribers
27 and sometimes between their own subscribers and those of other
28 networks. In addition, these service providers act as a gateway for
their subscribers to the Internet. Having said that, however, this
application does not seek to reach any host computers. This
application seeks permission only to search the SUBJECT
DEVICES specified in this affidavit and in Attachment A.

e. The Internet allows users, while still maintaining anonymity, to
easily locate (i) other individuals with similar interests in child
pornography, and (ii) websites that offer images of child
pornography. Those who seek to obtain images or videos of child
pornography can use standard Internet connections, such as those
provided by businesses, universities, and government agencies, to

1 communicate with each other and to distribute child pornography.
2 These communication links allow contacts around the world as
3 easily as calling next door. Additionally, these communications can
4 be quick, relatively secure, and as anonymous as desired. All of
5 these advantages, which promote anonymity for both the distributor
6 and recipient, are well known and are the foundation of transactions
7 involving those who wish to gain access to child pornography over
8 the Internet. Sometimes the only way to identify both parties and
9 verify the transportation of child pornography over the Internet is to
10 examine the distributor's/recipient's computer, including the Internet
11 history and cache to look for "footprints" of the websites and images
12 accessed by the distributor/recipient.

- 13 f. The computer's capability to store images in digital form makes it an
14 ideal repository for child pornography. The size of the electronic
15 storage media (commonly referred to as a "hard drive") used in
16 home computers has grown tremendously within the last several
17 years. Hard drives with the capacity of two terabytes are not
18 uncommon. These drives can store thousands of images at very high
19 resolution. Magnetic storage located in host computers adds another
20 dimension to the equation. It is possible to use a video camera to
21 capture an image, process that image in a computer with a video
22 capture board, and save that image to storage elsewhere. Once this is
23 done, there is no readily apparent evidence at the "scene of the
24 crime." Only with careful laboratory examination of electronic
25 storage devices is it possible to recreate and understand the evidence
26 trail.

27 42. Based upon my knowledge, experience, and training in child pornography
28 investigations, and the training and experience of other law enforcement officers with
whom I have had discussions, I know there are certain characteristics common to
individuals who have a sexualized interest in children and depictions of children:

- 29 a. They may receive sexual gratification, stimulation, and satisfaction
30 from contact with children; or from fantasies they may have viewing
31 children engaged in sexual activity or in sexually suggestive poses,
32 such as in person, in photographs, or other visual media; or from
33 literature describing such activity.

- 1 b. They may collect sexually explicit or suggestive materials in a
2 variety of media, including photographs, magazines, motion
3 pictures, videotapes, books, slides, and/or drawings or other visual
4 media. Such individuals often times use these materials for their own
5 sexual arousal and gratification. Further, they may use these
6 materials to lower the inhibitions of children they are attempting to
7 seduce, to arouse the selected child partner, or to demonstrate the
8 desired sexual acts. These individuals may keep records, to include
 names, contact information, and/or dates of these interactions, of the
 children they have attempted to seduce, arouse, or with whom they
 have engaged in the desired sexual acts.
- 9 c. They often maintain any “hard copies” of child pornographic
10 material that is, their pictures, films, video tapes, magazines,
11 negatives, photographs, correspondence, mailing lists, books, tape
12 recordings, etc., in the privacy and security of their home or some
13 other secure location, such as an office or safe. These individuals
14 typically retain these “hard copies” of child pornographic material
15 for many years, as they are highly valued.
- 16 d. Likewise, they often maintain their child pornography collections
17 that are in a digital or electronic format in a safe, secure and private
18 environment, such as a computer and its surrounding area. These
19 collections are often maintained for several years and are kept close
20 by, often at the individual’s residence or some otherwise easily
21 accessible location, to enable the owner to view the collection,
22 which is valued highly. They also may opt to store the contraband in
23 cloud accounts. Cloud storage is a model of data storage where the
24 digital data is stored in logical pools, the physical storage can span
25 multiple servers, and often locations, and the physical environment
26 is typically owned and managed by a hosting company. Cloud
27 storage allows the offender ready access to the material from any
28 device that has an Internet connection, worldwide, while also
 attempting to obfuscate or limit the criminality of possession as the
 material is stored remotely and not on the offender’s device.
- e. They also may correspond with and/or meet others to share
 information and materials; rarely destroy correspondence from other
 child pornography distributors/collectors; conceal such
 correspondence as they do their sexually explicit material; and often
 maintain lists of names, addresses, and telephone numbers of

1 individuals with whom they have been in contact and who share the
2 same interests in child pornography.

- 3 f. They generally prefer not to be without their child pornography for
4 any prolonged time period. This behavior has been documented by
5 law enforcement officers involved in the investigation of child
6 pornography throughout the world.

7 43. In addition to offenders who collect and store child pornography, law
8 enforcement has encountered offenders who obtain child pornography from the internet,
9 view the contents and subsequently delete the contraband, often after engaging in self-
10 gratification. In light of technological advancements, increasing Internet speeds and
11 worldwide availability of child sexual exploitative material, this phenomenon offers the
12 offender a sense of decreasing risk of being identified and/or apprehended with quantities
13 of contraband. This type of consumer is commonly referred to as a 'seek and delete'
14 offender, knowing that the same or different contraband satisfying their interests remain
15 easily discoverable and accessible online for future viewing and self-gratification. I know
16 that, regardless of whether a person discards or collects child pornography he/she
17 accesses for purposes of viewing and sexual gratification, evidence of such activity is
18 likely to be found on computers and related digital devices, including storage media, used
19 by the person. This evidence may include the files themselves, logs of account access
20 events, contact lists of others engaged in trafficking of child pornography, backup files,
21 and other electronic artifacts that may be forensically recoverable.

22 44. Given the above-stated facts, and based on my knowledge, training and
23 experience, along with my discussions with other law enforcement officers who
24 investigate child exploitation crimes, I believe that HERNANDEZ likely has a sexualized
25 interest in children and depictions of children, and that evidence of child pornography is
26 likely to be found on the SUBJECT DEVICES (based upon the images I have already
27 observed and the totality of the evidence above), specified in this affidavit and in
28 Attachment A.

1 45. Based on my training and experience, and that of computer forensic agents
2 that I work and collaborate with on a daily basis, I know that every type and kind of
3 information, data, record, sound or image can exist and be present as electronically stored
4 information on any of a variety of computers, computer systems, digital devices, and
5 other electronic storage media. I also know that electronic evidence can be moved easily
6 from one digital device to another. As a result, I believe that electronic evidence may be
7 stored on the SUBJECT DEVICES specified in this affidavit and in Attachment A.

8 46. Based on my training and experience, and my consultation with computer
9 forensic agents who are familiar with searches of computers, I know that in some cases,
10 the items set forth in Attachment B may take the form of files, documents, and other data
11 that is user-generated and found on a digital device. In other cases, these items may take
12 the form of other types of data – including in some cases data generated automatically by
13 the devices themselves.

14 47. Based on my training and experience, and my consultation with computer
15 forensic agents who are familiar with searches of computers, I believe there is probable
16 cause to believe that the items set forth in Attachment B will be stored in the SUBJECT
17 DEVICES set forth in this Affidavit and in Attachment A, for a number of reasons,
18 including but not limited to the following:

- 19 a. Once created, electronically stored information (ESI) can be stored
20 for years in very little space and at little or no cost. A great deal of
21 ESI is created, and stored, moreover, even without a conscious act
22 on the part of the device operator. For example, files that have been
23 viewed via the Internet are sometimes automatically downloaded
24 into a temporary Internet directory or “cache,” without the
25 knowledge of the device user. The browser often maintains a fixed
26 amount of hard drive space devoted to these files, and the files are
27 only overwritten as they are replaced with more recently viewed
28 Internet pages or if a user takes affirmative steps to delete them.
This ESI may include relevant and significant evidence regarding
criminal activities, but also, and just as importantly, may include
evidence of the identity of the device user, and when and how the
device was used. Most often, some affirmative action is necessary to

delete ESI. And even when such action has been deliberately taken, ESI can often be recovered, months or even years later, using forensic tools.

- b. Wholly apart from data created directly (or indirectly) by user-generated files, digital devices – in particular, a computer’s internal hard drive – contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible for a user to use such specialized software to delete this type of information – and, the use of such special software may itself result in ESI that is relevant to the criminal investigation. FBI agents in this case have consulted on computer forensic matters with law enforcement officers with specialized knowledge and training in computers, networks, and Internet communications. In particular, to properly retrieve and analyze electronically stored (computer) data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the computers. To effect such accuracy and completeness, it may also be necessary to analyze not only data storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the computer and software.

SEARCH AND/OR SEIZURE OF DIGITAL DEVICES

48. In addition, based on my training and experience and that of computer forensic agents that I work and collaborate with on a daily basis, I know that in most cases it is impossible to successfully conduct a complete, accurate, and reliable search for electronic evidence stored on a digital device during the physical search of a search site for a number of reasons, including but not limited to the following:

- a. Technical Requirements: Searching digital devices for criminal evidence is a highly technical process requiring specific expertise

1 and a properly controlled environment. The vast array of digital
2 hardware and software available requires even digital experts to
3 specialize in particular systems and applications, so it is difficult to
4 know before a search which expert is qualified to analyze the
5 particular system(s) and electronic evidence found at a search site.
6 As a result, it is not always possible to bring to the search site all of
7 the necessary personnel, technical manuals, and specialized
8 equipment to conduct a thorough search of every possible digital
9 device/system present. In addition, electronic evidence search
10 protocols are exacting scientific procedures designed to protect the
11 integrity of the evidence and to recover even hidden, erased,
12 compressed, password-protected, or encrypted files. Since ESI is
extremely vulnerable to inadvertent or intentional modification or
destruction (both from external sources and from destructive code
embedded in the system such as a "booby trap"), a controlled
environment is often essential to ensure its complete and accurate
analysis.

- 13 b. Volume of Evidence: The volume of data stored on many digital
14 devices is typically so large that it is impossible to search for
15 criminal evidence in a reasonable period of time during the
16 execution of the physical search of a search site. A single megabyte
17 of storage space is the equivalent of 500 double-spaced pages of
18 text. A single gigabyte of storage space, or 1,000 megabytes, is the
19 equivalent of 500,000 double-spaced pages of text. Computer hard
20 drives are now being sold for personal computers capable of storing
21 up to four terabytes (4,000 gigabytes of data.) Additionally, this
22 data may be stored in a variety of formats or may be encrypted
23 (several new commercially available operating systems provide for
24 automatic encryption of data upon shutdown of the computer).
- 25 c. Search Techniques: Searching the ESI for the items described in
26 Attachment B may require a range of data analysis techniques. In
27 some cases, it is possible for agents and analysts to conduct carefully
28 targeted searches that can locate evidence without requiring a time-
consuming manual search through unrelated materials that may be
commingled with criminal evidence. In other cases, however, such
techniques may not yield the evidence described in the warrant, and
law enforcement personnel with appropriate expertise may need to
conduct more extensive searches, such as scanning areas of the disk

1 not allocated to listed files, or peruse every file briefly to determine
2 whether it falls within the scope of the warrant.

3 49. In this particular case, and in order to protect the third party privacy of
4 innocent individuals, the following are search techniques that will be applied:

- 5 a. Use of hash value library searches.
- 6 b. Use of keyword searches, i.e., utilizing key words that are known to
7 be associated with the sharing of child pornography.
- 8 c. Identification of non-default programs that are commonly known to
9 be used for the exchange and viewing of child pornography, such as,
10 eMule, uTorrent, BitTorrent, Ares, Shareaza, Gnutella, etc.
- 11 d. Looking for file names indicative of child pornography, such as,
12 PTHC, PTSC, Lolita, 3yo, etc. and file names identified during the
undercover download of child pornography.
- 13 e. Viewing of image files and video files.
- 14 f. As indicated above, the search will be limited to evidence of child
15 pornography and will not include looking for personal documents
16 and files that are unrelated to the crimes listed in this Affidavit, or
17 those set forth in the original search warrant, MJ19-311.

18 50. These search techniques may not all be required or used in a particular
19 order for the identification of digital devices containing items set forth in Attachment B
20 to this Affidavit. However, these search techniques will be used systematically in an
21 effort to protect the privacy of third parties. Use of these tools will allow for the quick
22 identification of items authorized to be seized pursuant to Attachment B to this Affidavit,
23 and will also assist in the early exclusion of digital devices and/or files which do not fall
24 within the scope of items authorized to be seized pursuant to Attachment B to this
25 Affidavit.

26 **COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS**

27 51. Based on my knowledge, training, and experience, I know that digital
28 devices and electronic storage media can store information for long periods. Similarly,

1 things that have been viewed via the Internet are typically stored for some period of time
2 on the device used to access the Internet. This information can sometimes be recovered
3 with forensic tools.

4 52. There is probable cause to believe that things that were once stored on the
5 SUBJECT DEVICES may still be stored there, for at least the following reasons:

6 a. Based on my knowledge, training, and experience, I know that
7 computer files or remnants of such files can be recovered months or even years after they
8 have been downloaded onto a storage medium, deleted, or viewed via the Internet.
9 Electronic files downloaded to a storage medium can be stored for years at little or no
10 cost. Even when files have been deleted, they can be recovered months or years later
11 using forensic tools. This is so because when a person “deletes” a file on a computer, the
12 data contained in the file does not actually disappear; rather, that data remains on the
13 storage medium until it is overwritten by new data.

14 b. Therefore, deleted files, or remnants of deleted files, may reside in
15 free space or slack space—that is, in space on the storage medium that is not currently
16 being used by an active file—for long periods of time before they are overwritten. In
17 addition, a computer’s operating system may also keep a record of deleted data in a
18 “swap” or “recovery” file.

19 c. Wholly apart from user-generated files, computer storage media—in
20 particular, computers’ internal hard drives—contain electronic evidence of how a
21 computer has been used, what it has been used for, and who has used it. To give a few
22 examples, this forensic evidence can take the form of operating system configurations,
23 artifacts from operating system or application operation, file system data structures, and
24 virtual memory “swap” or paging files. Computer users typically do not erase or delete
25 this evidence, because special software is typically required for that task. However, it is
26 technically possible to delete this information.

27 d. Similarly, files that have been viewed via the Internet are sometimes
28 automatically downloaded into a temporary Internet directory or “cache.”

53. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT DEVICES were used, the purpose of its use, who used it, and when.

54. Manner of execution. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

SEARCH TECHNIQUES

55. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit imaging or otherwise copying all data contained on the SUBJECT DEVICES, and will specifically authorize a review of the media or information consistent with the warrant.

56. In accordance with the information in this affidavit, law enforcement personnel will execute the search of the SUBJECT DEVICES pursuant to this warrant as follows:

Securing the Data

a. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of the SUBJECT DEVICES.

b. Law enforcement will only create an image of data physically present on or within the SUBJECT DEVICES. Creating an image of the SUBJECT DEVICES will not result in access to any data physically located elsewhere. However, SUBJECT DEVICES that have previously connected to devices at other locations may contain data from those other locations.

1 **Searching the Forensic Images**

2 c. Searching the forensic images for the items described in Attachment
3 B may require a range of data analysis techniques. In some cases, it is possible for agents
4 and analysts to conduct carefully targeted searches that can locate evidence without
5 requiring a time-consuming manual search through unrelated materials that may be
6 commingled with criminal evidence. In other cases, however, such techniques may not
7 yield the evidence described in the warrant, and law enforcement may need to conduct
8 more extensive searches to locate evidence that falls within the scope of the warrant. The
9 search techniques that will be used will be only those methodologies, techniques and
10 protocols as may reasonably be expected to find, identify, segregate and/or duplicate the
11 items authorized to be seized pursuant to Attachment B to this affidavit.

12 d. These methodologies, techniques, and protocols may include the use
13 of a "hash value" library to exclude normal operating system files that do not need to be
14 further searched. Agents may utilize hash values to exclude certain known files, such as
15 the operating system and other routine software, from the search results. However,
16 because the evidence I am seeking does not have particular known hash values, agents
17 will not be able to use any type of hash value library to locate the items in Attachment B.

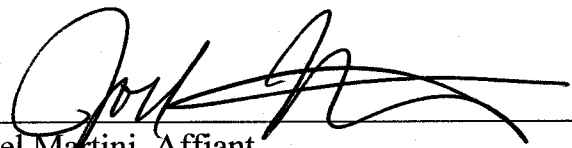
18 //

19 //

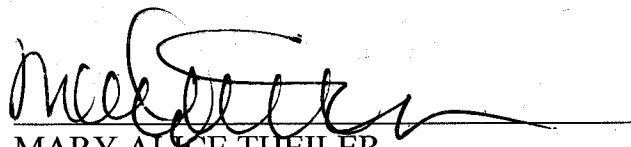
20 //

CONCLUSION

52. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) are located on the SUBJECT DEVICES set forth in this Affidavit and in Attachment A. I therefore request that the court issue a warrant authorizing a search of these items, as more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such evidence found therein.


Joel Martini, Affiant
Special Agent, Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me this 28 day of October, 2019.


MARY ALICE THEILER
United States Magistrate Judge

ATTACHMENT A**Description of Property to be Searched**

The property to be searched includes:

Item Description	FBI Evidence Number
1. One (1) HGST hard drive, S/N: 130325TEA45A3R240BK;	1B2
2. One (1) HGST hard drive, S/N: 130301E20342BM0V340S;	1B3
3. One (1) Hitachi hard drive, S/N: 111223E20B12C7CGL9RS;	1B4
4. One (1) Toshiba hard drive w/ power cord, G003250A;	1B5
5. One (1) Seagate hard drive w/enclosure, S/N: Z84112WS, S/N: NA8TLMTO;	1B8
6. Two (2) 4GB Powersticks, Model PSPV1;	1B10
7. One (1) Kodak memory card 8GB w/case, 31295-8GBCSTA;	1B14
8. One (1) ETC hotels thumb drive, 1GB 1011S;	1B15
9. One (1) ETC hotels thumb drive, 1GB 1011S;	1B16
10. One (1) Casa del Mar ETC hotel flashdrive 2GB;	1B17
11. One (1) Transcend Micro SD adapter 32GB, 9181AA32G09QS2;	1B18
12. One (1) Kingston Technologies hard drive 128GB, 50026B7726A02E6DE;	1B21
13. One (1) iPhone S, rose gold color, Model: A1633;	1B25
14. One (1) iPhone, black, Model: A1778;	1B28
15. One (1) Macbook w/power cord, S/N: C02MN8TDFD57;	1B32
16. One (1) iPhone X, black, cracked back	1B33

(collectively, the "SUBJECT DEVICES").

The SUBJECT DEVICES are currently being stored in the Federal Bureau of Investigation, Seattle Field Office, located at 1110 3rd Ave, Seattle, WA 98101.

This warrant authorizes the forensic examination of the SUBJECT DEVICES for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B
ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form, that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C.

§ 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C.

§ 2252(a)(4)(B) (Possession of Child Pornography), which may be found on the

SUBJECT DEVICES:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media.

2. Evidence of the installation and use of file-sharing software, and any associated logs, saved user names and passwords, shared files, and browsing history;

3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Evidence of who used, owned or controlled the SUBJECT DEVICES at the time the things described in this warrant were created, downloaded, viewed, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

7. Evidence of malware that would allow others to control any seized digital device(s) such as viruses, Trojan horses, and other forms of malicious software, as well

1 as evidence of the presence or absence of security software designed to detect malware;
2 as well as evidence of the lack of such malware;

3 8. Evidence of the attachment to the digital device(s) of other storage devices
4 or similar containers for electronic evidence;

5 9. Evidence of counter-forensic programs (and associated data) that are
6 designed to eliminate data from a digital device;

7 10. Evidence of times the digital device(s) was used;

8 11. Any other ESI from the digital device(s) necessary to understand how the
9 digital device was used, the purpose of its use, who used it, and when.

10 12. Records and things evidencing the use of:

11 a. Routers, modems, and network equipment used to connect
12 computers to the Internet;

13 b. Records of Internet Protocol (IP) addresses used;

14 c. Records of Internet activity, including firewall logs, caches, browser
15 history and cookies, "bookmarked" or "favorite" web pages, search terms that the user
16 entered into any Internet search engine, and records of user-typed web addresses.
17
18
19
20
21
22
23
24
25
26
27
28

EXHIBIT 1

Case 2:19-mj-02536-DUTY *SEALED* Document 1-1 *SEALED* Filed 06/18/19 Page 1 of 13

Page ID #:75

AO 93 (Rev. 11/13) Search and Seizure Warrant (USAO CDCA Rev. 04/17)

ORIGINAL

UNITED STATES DISTRICT COURT

for the
Central District of California

In the Matter of the Search of)
 (Briefly describe the property to be searched or identify the)
 person by name and address))
 40520 Aster Place, Palmdale, California 93551)

Case No. 2:19-MJ-02536

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

NOTE CHANGES MADE BY THE COURT

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Central District of California (identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

Such affidavit(s) or testimony are incorporated herein by reference.

YOU ARE COMMANDED to execute this warrant on or before 14 days from the date of its issuance (not to exceed 14 days)☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the U.S. Magistrate Judge on duty at the time of the return through a filing with the Clerk's Office.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____Date and time issued: June 18, 2019 @ 1:09 pm

Judge's signature

City and state: Los Angeles, CAHon. Maria A. Audero, U.S. Magistrate Judge

Printed name and title

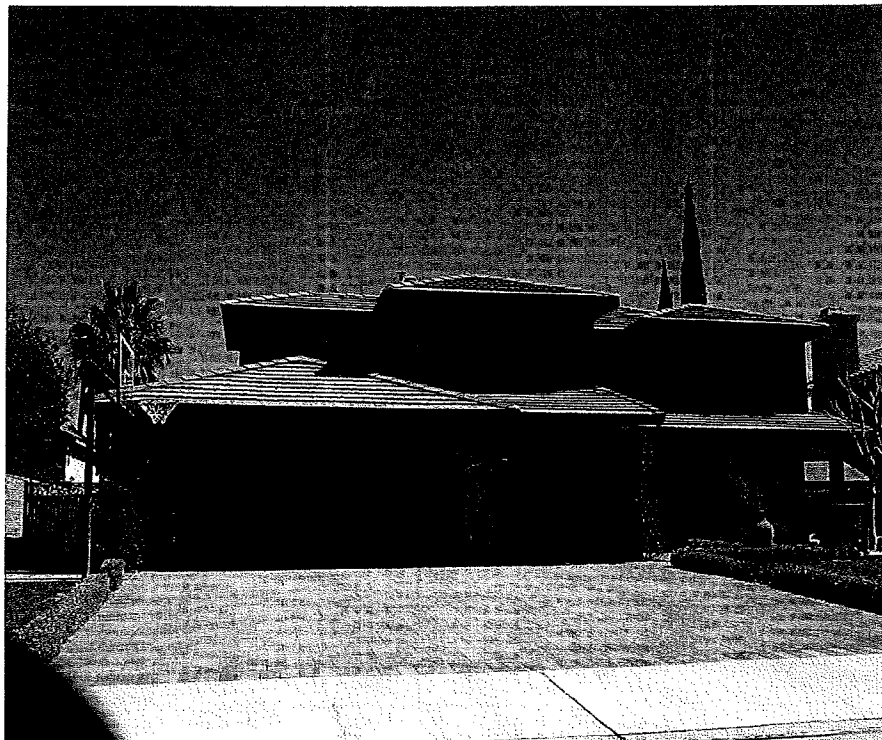
AUSA: Lisa Feldman (213)894-0633

Return		
Case No.: 2:19-MJ-02536	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized: 		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <p>Date: _____</p> <p style="text-align: right;">_____ <i>Executing officer's signature</i></p> <p style="text-align: right;">_____ <i>Printed name and title</i></p>		

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises to be search is located at **40520 Aster Place, Palmdale, California 93551** (the "**SUBJECT PREMISES**"). A photograph of the **SUBJECT PREMISES** is below:



The **SUBJECT PREMISES** is a two-story, single family dwelling, with tan-colored siding with brown trim and a brown tiled roof. The residence includes an attached garage containing two brown doors (two-car capacity and one-car capacity) separated by a multi-colored rock/stone pillar. The residence has single entry on the front and a black iron gate on the north side that leads to the back yard. There is a black in-ground basketball backboard located in front of the two-car

garage adjacent to the driveway. The driveway is constructed of multi-colored brick inlay and is lined on each side by small shrubs. The residence is located on the east side of Aster Place between Fairgreen Lane and Redbud Lane. The residence does not have a numbered address prominently displayed but is located on the same side of the street between 40528 Aster Place on the south and 40514 Aster Place on the north.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 371 and 1349 (Conspiracy), 1028(a)(7) (Identity Theft); 1028A (Aggravated Identity Theft); 1029(a)(2) (Access Device Fraud); 1030(a)(2), (4) and (5)(A) (Computer Fraud/Hacking); and 1343 (Wire Fraud) (the "Subject Offenses"), namely:

a. From January 2016 to the present: Records, documents, programs, applications or materials relating to any suspected attempt or plan to engage in computer hacking activity; access to computers or servers of Nintendo or to files, information, or data related to Nintendo products; the possession, use, or transfer of Nintendo authentication credentials, stolen property, or files, information, or data related to Nintendo or Nintendo products; research or reconnaissance about Nintendo products, release dates, or developer tools;

b. From January 2016 to the present: Records, documents, programs, applications, and materials relating to computer intrusions, hacking, malware, phishing, or any method to obscure or anonymize a person's identity;

c. Records, documents, programs, applications or materials relating to any prior contact with law enforcement, including the Federal Bureau of Investigation (FBI);

d. Records, documents, programs, applications or materials relating to any cease and desist notices or communications from Nintendo, Twitter or other business warnings against hacking;

e. Records, documents, programs, applications or materials relating to use of aliases or monikers, including but not limited to, the aliases "Ryan West" or "RyanRocks";

f. From January 2016 to the present: Records, documents, programs, applications or materials relating to use, or access to online accounts, including, but not limited to, email (e.g., Yahoo (Oath), Google), social media or networking (e.g., Twitter, Discord), cloud storage (e.g., Google Drive, iCloud) accounts;

g. Records, documents, programs, applications or materials relating to ownership of online accounts, including, but not limited to, email (e.g., Yahoo (Oath), Google), social media or networking (e.g., Twitter, Discord), cloud storage (e.g., Google Drive, iCloud) accounts;

h. Devices and software related to Nintendo products, including, but not limited to, developer kits (dev kits) and consoles, such as Nintendo 3DS and Switch;

i. Records, documents, programs, applications or materials relating to efforts to encrypt data or destroy evidence;

j. From January 2016 to the present: Records, documents, programs, applications or materials relating to communications with others regarding the suspected unauthorized

Case 2:19-mj-02536-DUTY *SEALED* Document 1-1 *SEALED* Filed 06/18/19 Page 7 of 13
Page ID #:81

transfer or possession of Nintendo data, files or property, and to the true identity of such persons;

k. From January 2016 to the present: Records, documents, programs, applications or materials relating to communications with Nintendo, its agents or representatives;

l. All records, documents, programs, applications or materials showing control, possession, custody or other indicia of occupancy over the **SUBJECT PREMISES**, or digital media found in the **SUBJECT PREMISES**, including but not limited to: personal mail, personal identification, bills, Internet service provider documents, rental documents, bank account documents, keys, or photographs;

m. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

n. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software,

as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

1. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The

government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime

was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling

outside the scope of the items to be seized absent further order of the Court.

2. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

- a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;
- b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;
- c. Any magnetic, electronic, or optical storage device capable of storing digital data;
- d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;
- e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;
- f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and
- g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

3. During the execution of this search warrant, law enforcement is permitted to: (1) ^{instruct} ~~depress~~ RYAN HERNANDEZ's ^{to depress his} thumb-
④ 4

and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of RYAN HERNANDEZ's face ^{and instruct him to hold} ~~with~~ his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

4. ^{executing the conditions of Paragraph 3 above} ~~In depressing a person's thumb or finger onto a device~~ and ~~in holding a device in front of a person's face,~~ law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

5. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

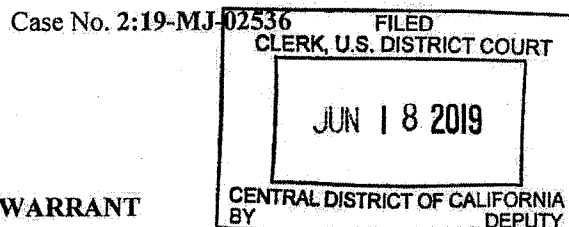
UNITED STATES DISTRICT COURT

for the
Central District of California

COPY

In the Matter of the Search of
(Briefly describe the property to be searched or identify the
person by name and address)

40520 Aster Place, Palmdale, California 93551



APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Central District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

18 U.S.C. §§371, 1349	Conspiracy
18 U.S.C. § 1028 (a) (7)	Identity Theft
18 U.S.C. § 1028A	Aggravated Identity Theft
18 U.S.C. § 1029 (a) (2)	Access Device Fraud
18 U.S.C. § 1030 (a) (2), (4) and (5)(a)	Computer Fraud/Hacking
18 U.S.C. § 1343	Wire Fraud

The application is based on these facts:

See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/
Applicant's signature

Joel Martini, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date:

June 18, 2019

MARIA A. AUDERO

Judge's signature

City and state: Los Angeles, CA

Hon. Maria A. Audero, U.S. Magistrate Judge

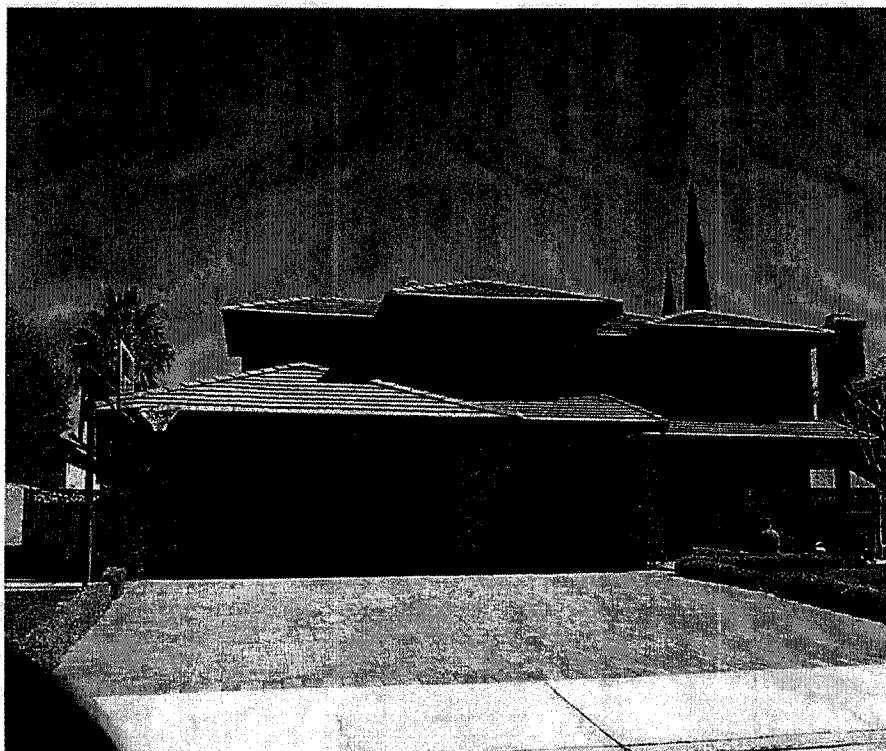
Printed name and title

AUSA: Lisa Feldman (213)894-0633

ATTACHMENT A

PREMISES TO BE SEARCHED

The premises to be search is located at 40520 Aster Place, Palmdale, California 93551 (the "SUBJECT PREMISES"). A photograph of the SUBJECT PREMISES is below:



The SUBJECT PREMISES is a two-story, single family dwelling, with tan-colored siding with brown trim and a brown tiled roof. The residence includes an attached garage containing two brown doors (two-car capacity and one-car capacity) separated by a multi-colored rock/stone pillar. The residence has single entry on the front and a black iron gate on the north side that leads to the back yard. There is a black in-ground basketball backboard located in front of the two-car

garage adjacent to the driveway. The driveway is constructed of multi-colored brick inlay and is lined on each side by small shrubs. The residence is located on the east side of Aster Place between Fairgreen Lane and Redbud Lane. The residence does not have a numbered address prominently displayed but is located on the same side of the street between 40528 Aster Place on the south and 40514 Aster Place on the north.

ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 371 and 1349 (Conspiracy), 1028(a)(7) (Identity Theft); 1028A (Aggravated Identity Theft); 1029(a)(2) (Access Device Fraud); 1030(a)(2), (4) and (5)(A) (Computer Fraud/Hacking); and 1343 (Wire Fraud) (the "Subject Offenses"), namely:

a. From January 2016 to the present: Records, documents, programs, applications or materials relating to any suspected attempt or plan to engage in computer hacking activity; access to computers or servers of Nintendo or to files, information, or data related to Nintendo products; the possession, use, or transfer of Nintendo authentication credentials, stolen property, or files, information, or data related to Nintendo or Nintendo products; research or reconnaissance about Nintendo products, release dates, or developer tools;

b. From January 2016 to the present: Records, documents, programs, applications, and materials relating to computer intrusions, hacking, malware, phishing, or any method to obscure or anonymize a person's identity;

c. Records, documents, programs, applications or materials relating to any prior contact with law enforcement, including the Federal Bureau of Investigation (FBI);

d. Records, documents, programs, applications or materials relating to any cease and desist notices or communications from Nintendo, Twitter or other business warnings against hacking;

e. Records, documents, programs, applications or materials relating to use of aliases or monikers, including but not limited to, the aliases "Ryan West" or "RyanRocks";

f. From January 2016 to the present: Records, documents, programs, applications or materials relating to use, or access to online accounts, including, but not limited to, email (e.g., Yahoo (Oath), Google), social media or networking (e.g., Twitter, Discord), cloud storage (e.g., Google Drive, iCloud) accounts;

g. Records, documents, programs, applications or materials relating to ownership of online accounts, including, but not limited to, email (e.g., Yahoo (Oath), Google), social media or networking (e.g., Twitter, Discord), cloud storage (e.g., Google Drive, iCloud) accounts;

h. Devices and software related to Nintendo products, including, but not limited to, developer kits (dev kits) and consoles, such as Nintendo 3DS and Switch;

i. Records, documents, programs, applications or materials relating to efforts to encrypt data or destroy evidence;

j. From January 2016 to the present: Records, documents, programs, applications or materials relating to communications with others regarding the suspected unauthorized

transfer or possession of Nintendo data, files or property, and to the true identity of such persons;

k. From January 2016 to the present: Records, documents, programs, applications or materials relating to communications with Nintendo, its agents or representatives;

l. All records, documents, programs, applications or materials showing control, possession, custody or other indicia of occupancy over the **SUBJECT PREMISES**, or digital media found in the **SUBJECT PREMISES**, including but not limited to: personal mail, personal identification, bills, Internet service provider documents, rental documents, bank account documents, keys, or photographs;

m. Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the Subject Offense/s, and forensic copies thereof.

n. With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software,

as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

2. As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified, or stored in any form, including in digital form on any digital device and any forensic copies thereof.

3. ~~As used herein,~~ the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, floppy disks, memory cards, optical disks, and magnetic tapes used to store digital data (excluding analog tapes such as VHS); and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICES

1. In searching digital devices or forensic copies thereof, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the "search team") will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location. The search team shall complete the search as soon as is practicable but not to exceed 120 days from the date of execution of the warrant. The

government will not search the digital device(s) and/or forensic image(s) thereof beyond this 120-day period without obtaining an extension of time order from the Court.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, "hidden," or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as "EnCase" and "FTK" (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime

was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling

outside the scope of the items to be seized absent further order of the Court.

2. In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

- a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;
- b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;
- c. Any magnetic, electronic, or optical storage device capable of storing digital data;
- d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;
- e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;
- f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and
- g. Any passwords, password files, biometric keys, test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.

3. During the execution of this search warrant, law enforcement is permitted to: (1) depress RYAN HERNANDEZ's thumb-

and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of RYAN HERNANDEZ's face with his or her eyes open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.

4. In depressing a person's thumb or finger onto a device and in holding a device in front of a person's face, law enforcement may not use excessive force, as defined in Graham v. Connor, 490 U.S. 386 (1989); specifically, law enforcement may use no more than objectively reasonable force in light of the facts and circumstances confronting them.

5. The special procedures relating to digital devices found in this warrant govern only the search of digital devices pursuant to the authority conferred by this warrant and do not apply to any search of digital devices pursuant to any other court order.

AFFIDAVIT

I, Joel Martini, being duly sworn, declare and state as follows:

INTRODUCTION

1. I am a Special Agent ("SA") with the Federal Bureau of Investigation (FBI), currently assigned to the Seattle Field Office, and have been so employed since January 2017. I am assigned to the Cyber squad where I primarily investigate computer intrusions and other Cybercrimes. My experience as an FBI Agent includes the investigation of cases involving the use of computers and the Internet to commit crimes. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, Cybercrimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. I have personally participated in the execution of search warrants involving the search and seizure of computer equipment. I have received advanced training in the acquisition and analysis of digital evidence (both network and host based), responding to computer intrusions and other incidents. I currently hold a Bachelor's of Science in Information Systems from Corban University.

2. Prior to my employment as a Special Agent, I worked as a Computer Forensic Examiner for the FBI for approximately 5 years. As part of that employment, I became familiar with the

design and operations of various electronic devices, networks, and websites, including technology described herein.

PURPOSE OF AFFIDAVIT

3. This affidavit is made in support of a search warrant for **40520 Aster Place, Palmdale, California 93551** (the "**SUBJECT PREMISES**") described in Attachment A, for the items to be seized described in Attachment B.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

PREMISES TO BE SEARCHED

5. As described in Attachment A, which is incorporated herein by reference, the **SUBJECT PREMISES** to be searched is described as follows: A two-story, single family dwelling, with tan-colored siding with brown trim and a brown tiled roof. The residence includes an attached garage containing two brown doors (two-car capacity and one-car capacity) separated by a multi-colored rock/stone pillar. The residence has single entry on the front and a black iron gate on the north side that leads to the back yard. There is a black in-ground basketball backboard located in front of the two-car garage adjacent to the driveway.

The driveway is constructed of multi-colored brick ~~inlay and is~~ lined on each side by small shrubs. The residence is located on the east side of Aster Place between Fairgreen Lane and Redbud Lane. The residence does not have a numbered address prominently displayed but is located on the same side of the street between 40528 Aster Place on the south and 40514 Aster Place on the north.

ITEMS TO BE SEIZED

6. The items to be seized are the evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 371 and 1349 (Conspiracy), 1028(a)(7) (Identity Theft); 1028A (Aggravated Identity Theft); 1029(a)(2) (Access Device Fraud); 1030(a)(2), (4) and (5)(A) (Computer Fraud/Hacking); and 1343 (Wire Fraud), as described in Attachment B, which is incorporated herein by reference.

SUMMARY OF PROBABLE CAUSE

7. The FBI Seattle Office is conducting an investigation into a data breach and network intrusions, having received information from Nintendo regarding unauthorized access to Nintendo computer systems and the subsequent theft and dissemination of confidential and proprietary data.

8. The FBI has identified the suspected hacker as RYAN HERNANDEZ, also known as "Ryan West" and "RyanRocks" ("HERNANDEZ"), an individual previously known to the FBI and to Nintendo for prior hacking conduct targeting Nintendo and its products.

9. HERNANDEZ, born in 1999, resides at 40520 Aster Place, Palmdale, California 93551 (**SUBJECT PREMISES**), with his parents (Ruben and Sheila Hernandez¹), and has done so at all times material to this investigation. As discussed in more detail below, the evidence shows that HERNANDEZ committed the data breach and network intrusions from the **SUBJECT PREMISES**, using computers, devices, and other instrumentalities located at the **SUBJECT PREMISES**. There is further probable cause to believe that the fruits of the criminal activity, for instance, stolen files and data exfiltrated from protected Nintendo computers, are located at the **SUBJECT PREMISES**.

10. Nintendo is a consumer electronics and video game company. Nintendo Co., Ltd, is headquartered in Japan, and its North American subsidiary, Nintendo of America, is located in Redmond, Washington. Nintendo has manufactured a variety of home and handheld game consoles, such as the Wii U, 3DS, and the Switch, and developed multiple popular video game franchises, such as Mario, The Legend of Zelda, Pokémon, Animal Crossing, and Splatoon, among others.

TERMS AND DEFINITIONS

11. For the purpose of this affidavit, I use the following terms as described below:

a. An Internet Protocol address, or simply "IP address," is a unique numeric address used by devices, such as computers, on the Internet. Every device attached to the

¹ Their names are relevant to probable cause as to the **SUBJECT PREMISES**, as described further below.

Internet must be assigned an IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Generally, a static IP address is permanently assigned to a specific location or device as opposed to a dynamic IP address that is temporary and periodically changes.

b. A server is a computer that provides services for other computers connected to it via a network or the Internet. The computers that use the server's services are sometimes called "clients." Servers can be physically located anywhere with a network connection that may be reached by the clients; for example, it is not uncommon for a server to be located hundreds (or even thousands) of miles away from the client computers. A server may be either a physical or virtual machine. A physical server is a piece of computer hardware configured as a server with its own power source, central processing unit or units and associated software. A virtual server is typically one of many servers that operate on a single physical server. Each virtual server shares the hardware resources of the physical server but the data residing on each virtual server is segregated from the data on other virtual servers that reside on the same physical machine.

c. A Content Delivery Network, or "CDN," refers to a method by which data is transmitted by using a system of distributed servers that deliver the content based on your geographic location. This helps speed up data transfer.

d. A Local Area Network, or "LAN," typically refers to a group of interconnected computers.

e. The Onion Router, or "Tor," is an anonymity tool used by individuals when they wish to obfuscate the origin of the internet connection (entry point). This is accomplished by bouncing the original internet connection through several intermediate computers (relays) that utilize encryption, thus anonymizing the entry point.

f. Malware is malicious computer code running on a computer. Malware can be designed to do a variety of things, including logging every keystroke on a computer, stealing financial information or "user credentials" (passwords or usernames), or commanding that computer to become part of a network of "robot" or "bot" computers known as a "botnet." In addition, malware can be used to transmit data from the infected computer to another destination on the Internet, as identified by an IP address.

g. Phishing is a deceptive technique in which the perpetrators use messages and/or fake websites to trick people into providing information, such as network credentials (e.g., user names and passwords) that may later be used to gain access to the victim's systems.

h. A "botnet" typically refers to a network of compromised computers known as "bots" that are under the control of a cybercriminal or "bot herder." The bots are harnessed by the bot herder through the surreptitious installation of malware that provides the bot herder with remote access to, and control

of, the compromised computers. A botnet may be used en masse, in a coordinated fashion, to deliver a variety of Internet-based attacks, including DDoS attacks, brute force password attacks, the transmission of spam emails, the transmission of phishing emails, and hosting communication networks for cybercriminals (e.g., acting as a proxy server for email communications).

STATEMENT OF PROBABLE CAUSE

A. HERNANDEZ's History of Targeting Nintendo²

12. As noted herein, HERNANDEZ is an individual previously known to Nintendo for having repeatedly targeted Nintendo and its products. Below I describe two instances --- the first of which was described to investigators by Nintendo representatives, and the second of which I was personally involved as part of a criminal investigation.

1. 2016 Abuse of Nintendo Developer Portal and Dissemination of Confidential Information

13. The following information was conveyed to me by Nintendo in communications in 2018 and 2019.

14. In 2016, HERNANDEZ registered online for Nintendo developer access, which, among other things, required that he accept the terms of a non-disclosure agreement governing the use and disclosure of information. The Developer Portal is an online resource intended for individuals' legitimate use in developing products in association with Nintendo products.

² In this section, except where noted, I learned this information from documents provided by Nintendo or communications with representatives of Nintendo in 2018 and 2019.

15. Without authorization from Nintendo, HERNANDEZ then accessed confidential and proprietary information, including material for the Wii U console and Nintendo 3DS system, through Nintendo's online developer sites. HERNANDEZ then, in violation of the terms of the non-disclosure agreement and various laws, publicly posted and disclosed such information. Such disclosures of confidential and proprietary information increase the risk of piracy of Nintendo products, among other harms caused to Nintendo.

16. Nintendo, through its representative, later contacted HERNANDEZ demanding he cease and desist such conduct. HERNANDEZ, then a minor, and his parents agreed that HERNANDEZ would cease such activities and cease use of Nintendo's developer sites and confidential and proprietary information by signing a settlement agreement with Nintendo on September 30, 2016.

2. 2016-2017 Hack of Nintendo Developer Portal and Dissemination of Confidential Information

17. Despite that September 2016 agreement, HERNANDEZ thereafter engaged in similar hacking activity targeting Nintendo and stole its confidential and proprietary information, which led to a criminal referral by Nintendo and subsequent initiation of an FBI investigation into HERNANDEZ's hacking activity. Based on my involvement in that investigation, I learned the following, set forth below.

18. In March 2017, Nintendo contacted FBI Seattle regarding a network intrusion and reported the following:

a. In about October 2016, a user on Nintendo's online Developer Portal (later identified as HERNANDEZ) successfully persuaded a Nintendo employee to respond to a help request posted (by HERNANDEZ) on a Nintendo online forum. The post was, in reality, a phishing attempt, which contained a link directing the user to an external site hosting a malware program designed to secretly log the user's information.

b. Upon clicking on the link in the post, the Nintendo employee's Developer Portal credentials were hijacked and forwarded to a malicious subject (later identified as HERNANDEZ).

c. The malicious subject (later identified as HERNANDEZ) then used the employee's stolen account credentials to upload malware onto the Nintendo developer site, which logged the tokens of legitimate users logging onto the site, and later to gain administrator access³ to the Developer Portal and download proprietary Nintendo data.

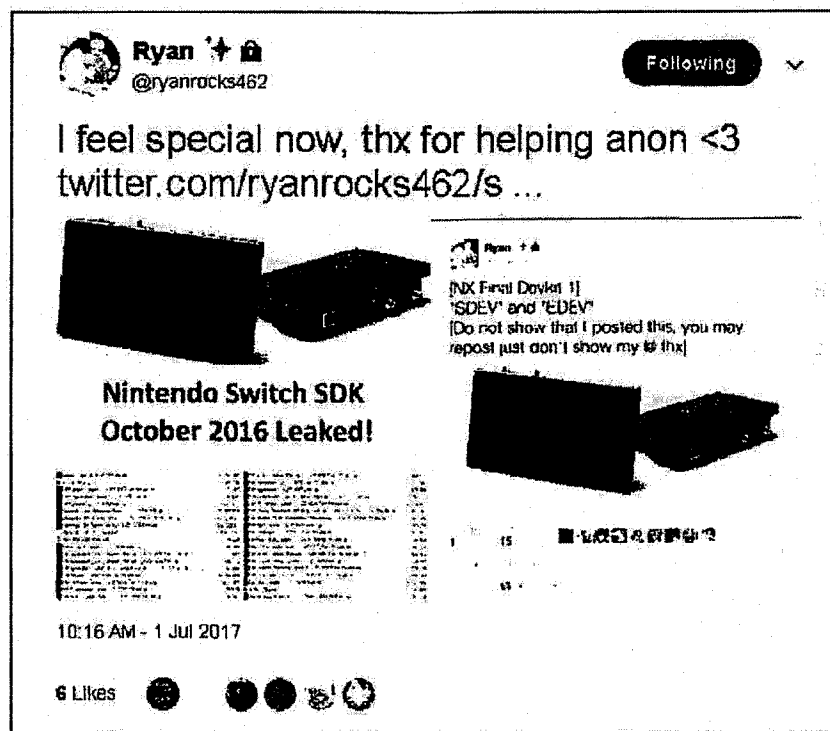
19. Nintendo launched an internal investigation into the incident and identified the malicious subject as HERNANDEZ. Nintendo made this identification, in part, by matching the IP address (172.248.227.193) used for the attack with the IP address legitimately used by HERNANDEZ on the Nintendo network.

20. Further, Nintendo noticed that some of the stolen data was appearing on a Twitter account with the username

³ Administrator access means a user has privileges to perform most, if not all, functions within an operating system on a computer.

Case 2:19-mj-02536-DUTY *SEALED* Document 1 *SEALED* Filed 06/18/19 Page 22 of 74
Page ID #:22

@ryanrocks462 ("TWITTER ACCOUNT 1"). Nintendo also provided FBI with copies of Twitter posts from user @ryanrocks462 (TWITTER ACCOUNT 1) implying responsibility for publicly leaking Nintendo information. For instance, in July 2017, Twitter user @ryanrocks462 (TWITTER ACCOUNT 1) appeared to take credit for the leak of data related to the Nintendo Switch SDK, while thanking "anon" for assistance:



As discussed below, FBI later confirmed that TWITTER ACCOUNT 1 belonged to HERNANDEZ.

21. FBI Seattle opened an investigation and confirmed through legal process that IP address 172.248.227.193 (hereinafter, "HERNANDEZ HOME IP #1") was HERNANDEZ's static IP address at his Palmdale, California Residence (SUBJECT PREMISES) at that time.

22. More specifically, I reviewed records obtained from Charter Communications, the service provider for IP address 172.248.227.193 (HERNANDEZ HOME IP #1). The account for HERNANDEZ HOME IP #1 was activated in December 2015 in the name of "Ruben Hernandez" (HERNANDEZ's father) at the **SUBJECT PREMISES**, as set forth below:⁴

Target Details	172.248.227.193, 9/9/2016 12:01:00 AM, GMT, 0
Subscriber Name:	RUBEN HERNANDEZ
Subscriber Address:	40520 ASTER PL, PALMDALE, CA 93551-2508
Service Type - RR HSD	Activate Date: 12/14/2015 Deactivate Date: Still Active
User Name or Features:	[REDACTED]
Phone number:	[REDACTED]
Advanced Subscriber Info	
Account Number:	[REDACTED]
Equipment Details	
MAC:	d405983403e2
Other Details	
Other Information:	IP Lease Information: First seen: 1/14/2016 1:06:52 PM Through 6/10/2017 1:26:52 AM

3. On October 25, 2017, FBI Agents Met with HERNANDEZ and His Parents at the SUBJECT PREMISES Regarding the Hacking Scheme and Once Again, HERNANDEZ Agreed to Stop

23. On about October 25, 2017, FBI agents (including this affiant) met with and interviewed HERNANDEZ at his Palmdale, California residence (**SUBJECT PREMISES**).⁵ Also present were HERNANDEZ's parents, Ruben and Sheila Hernandez. HERNANDEZ confirmed that he used Twitter account @ryanrocks462 (TWITTER ACCOUNT 1) but initially claimed that his posts about hacking

⁴ Some of Ruben Hernandez's personal information has been redacted for his privacy.

⁵ During the interview, HERNANDEZ responded to investigators' questions predominantly in writing and through gestures. According to his father, HERNANDEZ was seeing specialists for developmental difficulties.

Nintendo were simply jokes. After initially denying involvement in the Nintendo hack, HERNANDEZ acknowledged accessing the Nintendo Developer Portal, but claimed he did so at the direction of an unknown anonymous Twitter user who had since deleted his/her account. HERNANDEZ also claimed to have deleted any Nintendo data. At the conclusion of the interview, HERNANDEZ promised to stop any further malicious activity against Nintendo and indicated an understanding of potential consequences of future criminal activity.

24. Based on my involvement in this investigation, I believe that HERNANDEZ was severely minimizing his role in the prior hack of Nintendo and theft of property. As discussed below, based on evidence FBI has gathered through the current investigation, it appears that HERNANDEZ was the primary hacker who was assisted by an unidentified co-conspirator, believed to be the "anon" referenced in the Twitter post about the Nintendo Switch SDK data leak, depicted above.

C. Summary of Current Investigation

25. As discussed below, in 2018, despite his promises -- twice (2016 and 2017) -- to cease attacking Nintendo and its products, HERNANDEZ again hacked Nintendo's networks and successfully compromised numerous servers, located in Western Washington and elsewhere. Nintendo confirmed that, according to its internal investigation and ongoing remediation efforts, HERNANDEZ continues to maintain access to various server groups and has exfiltrated confidential and proprietary information.

26. As discussed below, Nintendo has provided the FBI with network logs and other information related to the intrusion as well as additional material related to its hacking investigation of HERNANDEZ.

27. As further discussed below, I and other investigators have conducted follow-up investigation and also identified HERNANDEZ as the perpetrator of the hacking scheme.

28. According to Nintendo, the internal investigation and remediation efforts remain ongoing. According to Nintendo's preliminary assessment, the intrusion has affected numerous computers and servers and caused a significant but yet determined amount of loss.

1. Referral and Investigation by Nintendo of Hacking Activity by HERNANDEZ

29. In October 2018, Nintendo again contacted FBI Seattle to report further network intrusion activity, which it attributed to HERNANDEZ. Below summarizes information provided to investigators by Nintendo.

30. Nintendo observed a hacker using HERNANDEZ HOME IP #1 (172.248.227.193) -- previously identified as associated with HERNANDEZ and the **SUBJECT PREMISES** in conjunction with the 2016-2017 developer portal hack --- using an unauthorized authentication certificate to access various internal Nintendo development tools and unreleased game titles, among other things. Nintendo provided the FBI with various identifiers and accounts associated with HERNANDEZ. According to Nintendo, its internal examination of its network and remediation efforts

ultimately uncovered HERNANDEZ's unauthorized access to multiple Nintendo servers dedicated to various stages of product development and distribution, dating back to at least June 2018.

31. Based on the referral and information provided, FBI opened a criminal investigation, which is described in more detail below.

a. Details about the Intrusion Activity and Background Information of HERNANDEZ Provided by Nintendo

32. In January 2019, and thereafter, Nintendo representatives provided FBI additional details about the recent network intrusion and Nintendo's ongoing remediation efforts. Nintendo also provided additional information about its prior dealings with HERNANDEZ, including the 2016 conduct, discussed above.

33. Nintendo communicated locating unauthorized network access by HERNANDEZ HOME IP #1 (172.248.227.193) and more recently, beginning in about late-November 2018, by IP address 76.232.194.142, which Nintendo believed was also used by HERNANDEZ. As discussed below, IP address 76.232.194.142 (hereinafter, "HERNANDEZ HOME IP #2") was identified as HERNANDEZ's new home IP address.

34. According to Nintendo, as of January 2019, it had located evidence of HERNANDEZ's unauthorized access to at least four server groups. For example:

a. One of the server groups related to a staging environment for the Nintendo eShop, which was used for pre-production testing. In June 2018, the HERNANDEZ HOME IP #1

(172.248.227.193) accessed the servers, which required use of a legitimate certificate.⁶ The hacker (HERNANDEZ) requested pre-release information and downloaded data, including development tools and retail titles Splatoon 2 and Minecraft.

b. Similarly, in June 2018, HERNANDEZ HOME IP #1 (172.248.227.193) accessed the device authentication server group using an illegitimate certificate.

c. Beginning in July 2018, HERNANDEZ's IP address accessed the server group that managed content for Nintendo retail kiosks, including advertising material and game demos. Nintendo suspected that the certificates required from such access were possibly obtained from an application extracted from the previously compromised staging environment server group.

d. The impacted computers included servers located in the Western District of Washington, and elsewhere.

35. As part of its referral, Nintendo also provided the FBI with information it had gathered about HERNANDEZ and his activity relating to Nintendo and its products.⁷ HERNANDEZ maintains a large number and wide variety of accounts at various service providers, including YouTube, GitHub, Google, Apple, Yahoo (Oath Holdings, Inc.), Microsoft, BitBucket, Instagram, Facebook, Twitter, and Discord, among others. Such accounts

⁶ According to Nintendo, it observed other unauthorized actors using the same credentials, which led it to believe that the particular compromised credentials had been shared on some online forum or group.

⁷ Nintendo retains a third-party company to assist in monitoring and investigating threat activity and suspected hackers.

include, among others, HERNANDEZ's various Yahoo accounts, namely, ryanrocks462@yahoo.com (hereinafter, "YAHOO ACCOUNT 1"), ryanrocks562@yahoo.com (hereinafter, "YAHOO ACCOUNT 2"), and ryanrocks463@yahoo.com (hereinafter, "YAHOO ACCOUNT 3"); Twitter accounts, namely, username "@ryanrocks462" (TWITTER ACCOUNT 1) and username "@ryanrocks562" (hereinafter, "TWITTER ACCOUNT 2"); and Discord account, namely, username "ryanrocks462", and his Discord server called "Ryan's Underground Hangout" (hereinafter, "HERNANDEZ DISCORD SERVER").⁸

b. Samples of HERNANDEZ's Online Posts Related to Nintendo and Hacking Activity Provided by Nintendo

36. According to material Nintendo provided to investigators, which I have personally reviewed, HERNANDEZ openly discussed Nintendo and Nintendo products and his theft of Nintendo property through various online accounts, including Discord and Twitter. Some examples are set forth below.

i. HERNANDEZ's Discussions on Discord

37. Nintendo provided the FBI with screenshots and summaries of various posts by Discord user "ryanrocks462" (HERNANDEZ) on HERNANDEZ DISCORD SERVER, called "Ryan's Underground Hangout," gathered through its investigation.

38. Discord is social media service that basically enables users to create chatrooms (called "servers") where users can

⁸ As discussed below, investigators have conducted subsequent investigation regarding numerous accounts used by HERNANDEZ and located evidence of criminal activity.

communicate through posts and/or direct messages as well as through voice or video chat.⁹

39. HERNANDEZ DISCORD SERVER also had various "channels," which are akin to topic-specific message boards or chats, which included such names as #nintendo-switch-keys, #switch-title-keys, #hacky-talk, #splatoon-2-talk, #splatoon-1-shit, among several others.

(I) HERNANDEZ's Discord Posts Regarding Nintendo and Hacking-Related Activity

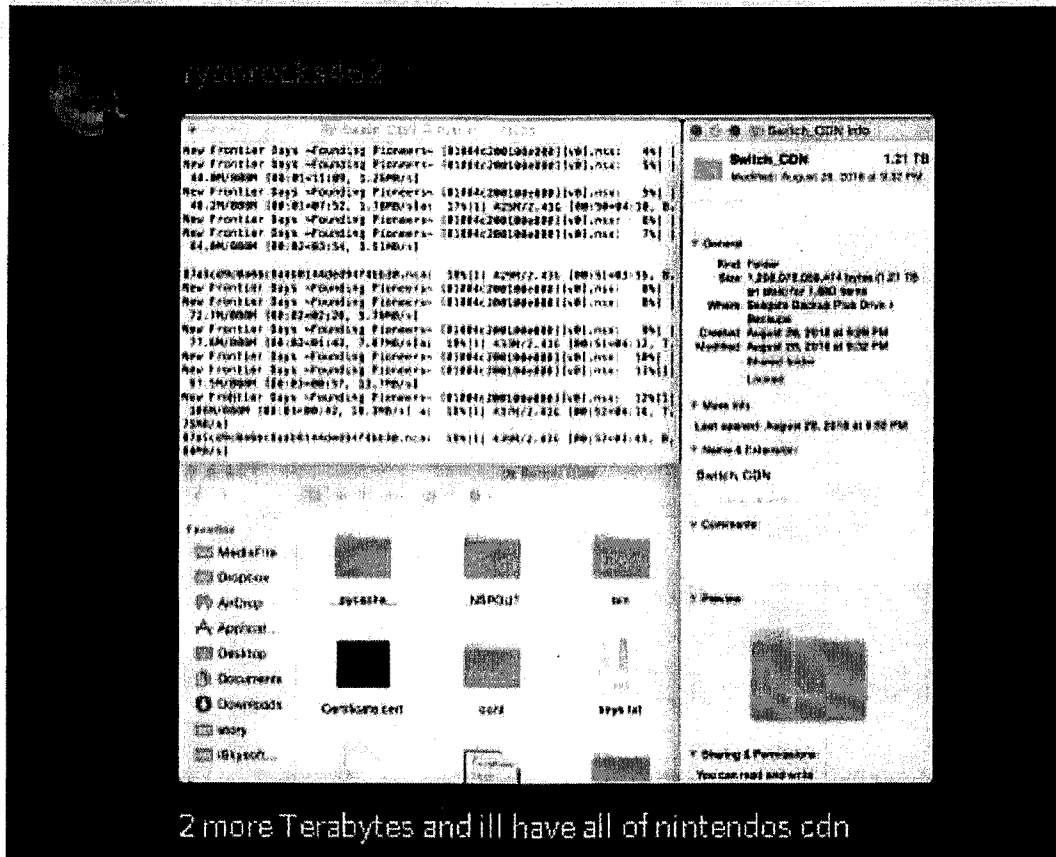
40. Discord user "ryanrocks462" (HERNANDEZ) posted on Ryan's Underground Hangout" (HERNANDEZ DISCORD SERVER) numerous messages suggesting he was engaged in hacking activity and had unauthorized access to files and information pertaining to Nintendo products.¹⁰ Below are several examples:

a. Discord user "ryanrocks462" (HERNANDEZ) claimed to have access to Nintendo servers and was actively downloading content, specifically related to the Nintendo Switch. For

⁹ A Discord "server" can be configured as public, meaning anyone can join, or it can be configured to be private. To participate in a private server, a user must be invited by another user who already belongs to that private server. Invitations can be configured to expire after a short period of time, limited to the number of times an invitation can be shared, and even be configured to limit a user to participating in the group one time.

¹⁰ The sample screenshots and summaries of Discord postings described herein were provided to FBI by Nintendo and occurred on Ryan's Underground Hangout" (HERNANDEZ DISCORD SERVER). It is believed that HERNANDEZ participates on other servers as well. For instance, according to the material provided by Nintendo, in October 2018, Discord user "ryanrocks462" (HERNANDEZ) posted an invitation to another Discord server called "WarezNX," which is believed to also relate to Nintendo products.

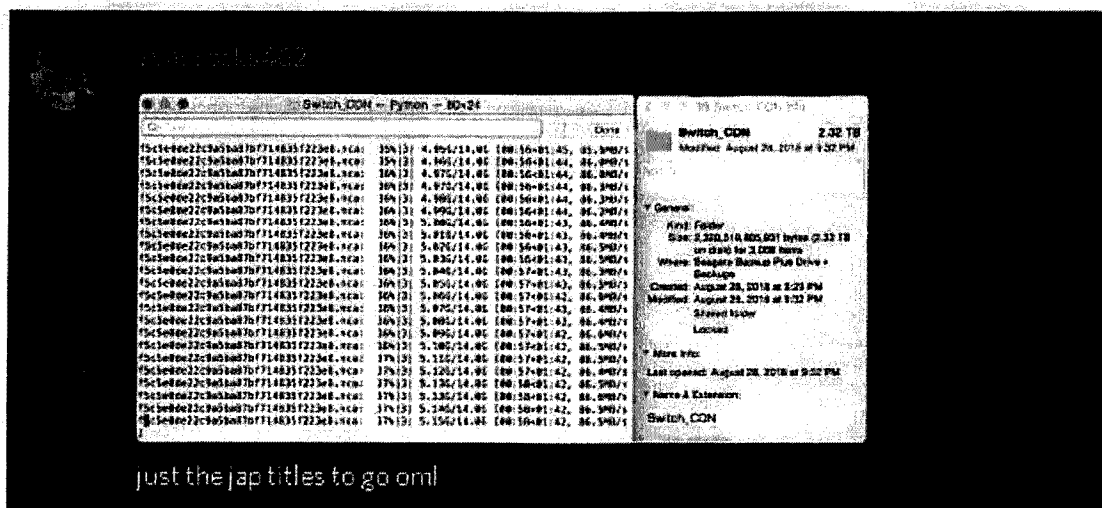
instance, on August 28, 2018, "ryanrocks462" (HERNANDEZ) posted a screenshot of what appears to be a file folder titled "Switch_CDN" along with the message: "2 more Terabytes and ill have all of nintendos cdn":



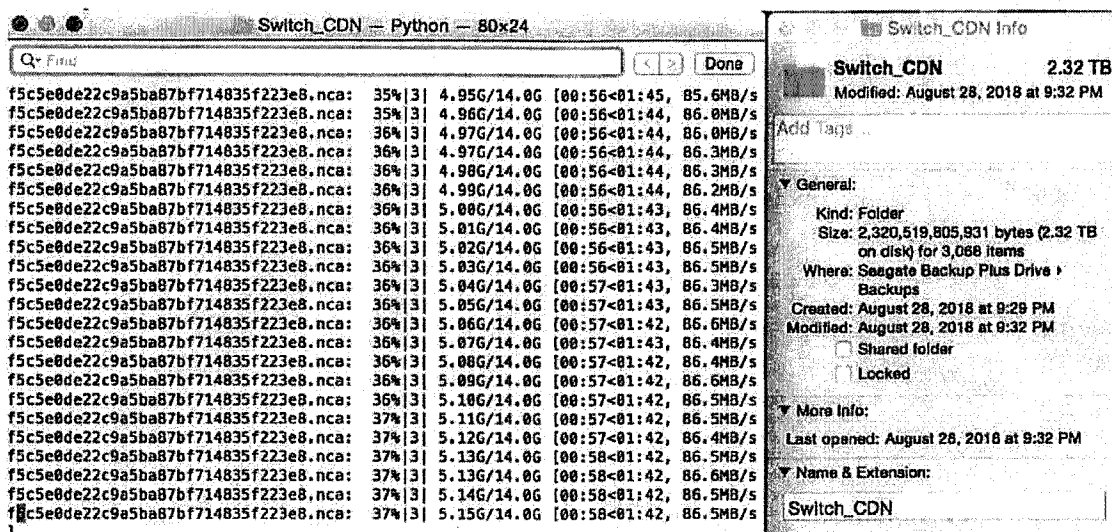
Based on my training and experience and knowledge of this investigation, I believe that in the above post, HERNANDEZ indicated that he was in the process of downloading Nintendo files.

b. On about September 3, 2018, Discord user "ryanrocks462" (HERNANDEZ) posted a similar image of the "Switch_CDN" file folder with the message: "just the jap titles

to go oml":¹¹



just the jap titles to go oml



Based on my training and experience and knowledge of this investigation, I believe that in the above post, HERNANDEZ provided an update regarding his downloading Nintendo files. I also noticed that the "Switch_CDN" folder appears to contain

¹¹ According to various online reference sites, "oml" typically means "Oh My Lord" in Internet slang. The term "jap" is a slang term for Japanese. As mentioned above, Nintendo Co., Ltd, is a Japanese company and markets games to numerous markets worldwide, including in Japan.

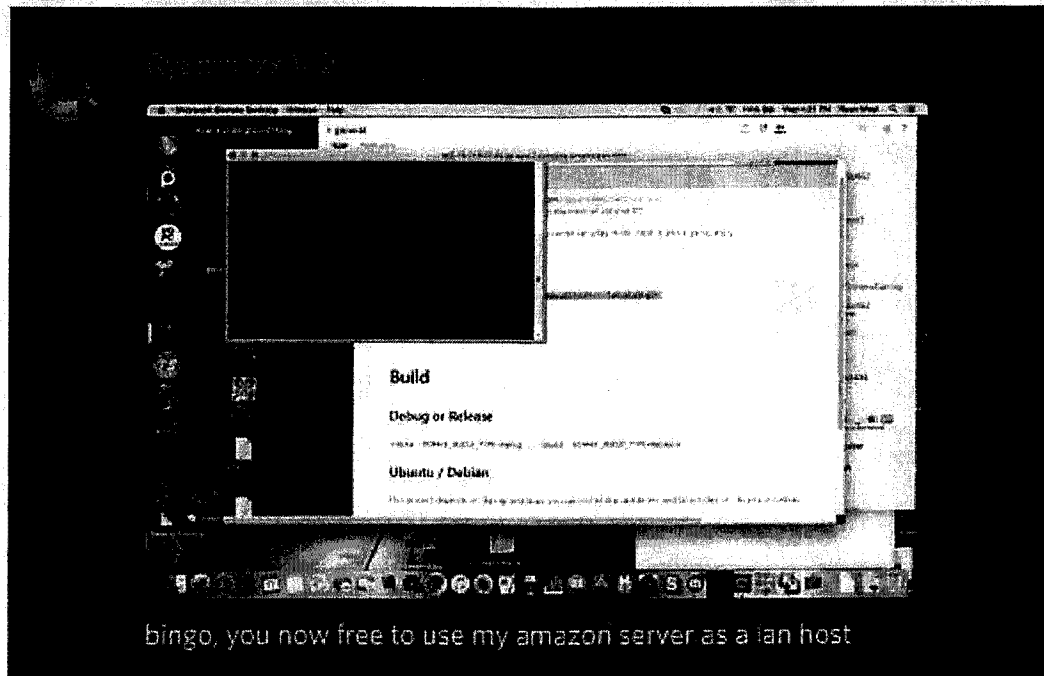
c. On September 24, 2018, Discord user

the new botnet server :))))))

d. On October 17, 2018, Discord user "ryanrocks462"

20

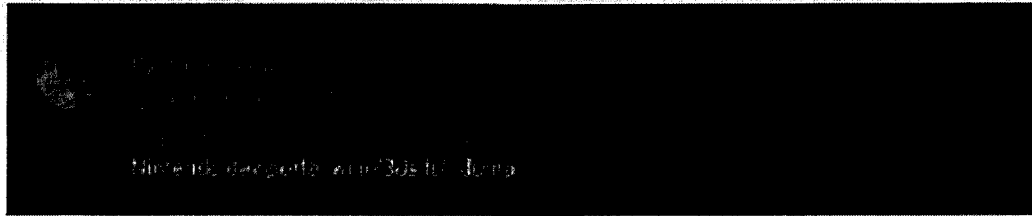
allowed to use his Amazon server as a LAN host:



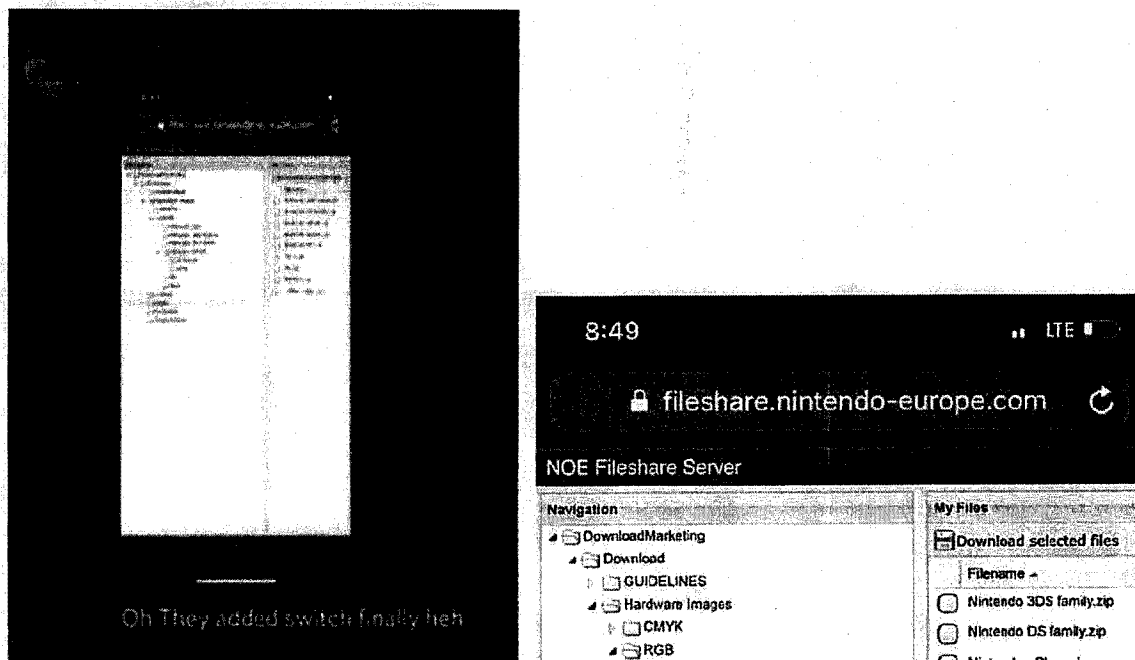
According to information provided by Nintendo, based on my training and experience, review of the image indicates Discord user "ryanrocks462" (HERNANDEZ) appears to be running a Switch play LAN host, which allows others to access Nintendo games and products.

e. On December 12, 2018, Discord user "ryanrocks462" (HERNANDEZ) posted a link to Google Drive that he claimed contained the Nintendo Developer Portal for Wii U and 3DS:¹²

¹² According to information provided by Nintendo, the owner of the Google Drive folder was listed as [M.L.]; the name is being redacted because M.L. is not a suspect at this time.



f. On December 16, 2018, Discord user "ryanrocks462" (HERNANDEZ) posted an image of the file directory on files.nintendo-europe.com and commented that the Switch had been added. The image appears to have been taken via a cellphone.



Based on my training and experience and knowledge of this investigation, I believe that this post suggests that HERNANDEZ may have access to a Nintendo file directory, related to the Nintendo 3DS and Switch consoles, among other things.

g. On January 20, 2019, Discord user "ryanrocks462"

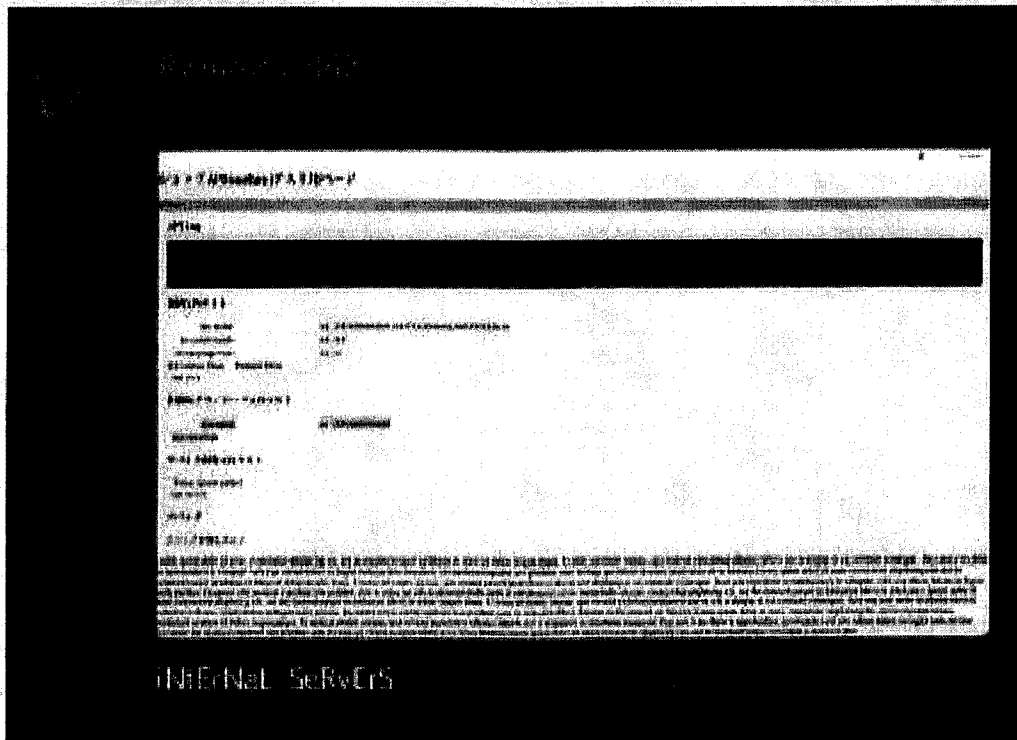
(HERNANDEZ) posted a screenshot of a file directory, which appears to relate to Splatoon 2, a Nintendo product, along with the message: "lg [large] I should get to work uwu"¹³:

Name	Date Modified	Size	Kind
Rockenberg H.S. caught bullying the innocent 1 RP Muzi	Jan 9, 2018, 8:18 AM	--	Folder
Screen Shot 2018-04-03 at 2:22:18 PM.png	May 9, 2018, 2:22 PM	5.6 MB	PNG image
Splatoon Hacks - all main weapons rapid fire onfire	Jul 3, 2017, 12:47 AM	--	Folder
Splatoon 2 - Squidlike Commercial voice over	Mar 3, 2018, 5:45 PM	--	Folder
Splatoon 2 Hacks - Accessing the Splatoon World Premiere in 2018	Mar 27, 2018, 3:22 AM	--	Folder
Splatoon 2 hacks - ancho v games early - force modes	Jul 20, 2018, 3:20 PM	--	Folder
Splatoon 2 Hacks - Camp Triggerfish early Rainmaker	Apr 13, 2018, 12:23 AM	--	Folder
Splatoon 2 Hacks - Camp Triggerfish Early Tower Control	Apr 3, 2018, 11:22 AM	--	Folder
Splatoon 2 Hacks - DLC Octoling early	May 6, 2018, 6:21 PM	--	Folder
Splatoon 2 Hacks - Equipped Hidden Octoling Gear with DLC Octo expansion octoling	May 9, 2018, 1:22 PM	--	Folder
Splatoon 2 Hacks - Equipped Charger and Agent 3 Gear in Turf War / Ranked Battles	Oct 12, 2018, 8:51 PM	--	Folder
Splatoon 2 Hacks - Mario's Character and Pocket Squid in Turf War / Ranked Battles	Sep 16, 2018, 7:31 AM	--	Folder
oktopen	Sep 27, 2018, 7:18 PM	18 KB	XML text
Original Recordings	Sep 27, 2018, 3:12 AM	--	Folder
Screen Shot 2018-09-27 at 3:29:31 PM.png	Sep 27, 2018, 3:29 PM	1.3 MB	PNG image
Screen Shot 2018-09-27 at 6:50:17 PM.png	Sep 27, 2018, 6:50 PM	5.8 MB	PNG image
Screen Shot 2018-09-27 at 6:50:34 PM.png	Sep 27, 2018, 6:50 PM	3.9 MB	PNG image
Screen Shot 2018-09-27 at 6:51:49 PM.png	Sep 27, 2018, 6:51 PM	4.2 MB	PNG image
splatoon 2 hacks.mov	Sep 27, 2018, 5:29 PM	3.05 GB	QT movie
thumbnail.jpg	Sep 27, 2018, 6:58 PM	907 KB	JPEG image
thumbnail.png	Sep 27, 2018, 6:58 PM	6.3 MB	PNG image
Splatoon 2 hacks - octoling in storymode	Mar 14, 2018, 8:16 PM	--	Folder
Splatoon 2 hacks - Piranha Plt Early Rainmaker	Mar 27, 2018, 3:35 AM	--	Folder
Splatoon 2 Hacks - Piranha Plt early Turf War	Mar 29, 2018, 11:30 AM	--	Folder
Splatoon 2 Hacks - Private battle with one person	Sep 22, 2018, 11:47 PM	--	Folder
Splatoon 2 Hacks - Brighthouse and Octoling bots in Offline Turf War / Ranked battle	Sep 19, 2018, 4:23 PM	--	Folder
Splatoon 2 Hacks - Turf War on Rainmaker Run	Apr 7, 2018, 8:17 AM	--	Folder
Splatoon 2 Hacks - Warao World early Rainmaker	May 31, 2018, 12:56 PM	--	Folder
Splatoon 2 Hacks - Warao World early Tower Control	May 31, 2018, 1:42 PM	--	Folder
Splatoon 2 Hacks ONLINE 1 - New Allscore Hotel Early INTENSE CLAM BUTZ! Ranked Battle!	Jun 28, 2018, 10:56 PM	--	Folder
Splatoon 2 OST Beginning a Match Different Versions Comparison	Jul 18, 2017, 12:54 PM	--	Folder
Splatoon 2 OST New or Older Different Versions Comparison	Jul 10, 2017, 10:26 AM	--	Folder
Splatoon 2 tutorial stage100 percent linked	Nov 9, 2017, 4:10 AM	--	Folder
Splatoon Demo Game Play [INTERACTIVE DEMO W6 U Kiosk]	May 28, 2017, 4:12 PM	--	Folder
Splatoon Hacks - Giving all Players Bots a Rainmaker in Offline Ranked Battle - VSGame	Aug 28, 2017, 11:59 AM	--	Folder
Splatoon Hacks - Ink Coverage Range Modifier	Jul 3, 2017, 1:52 AM	--	Folder
Splatoon Hacks - Online Plaza Modifier	Jan 30, 2017, 7:10 PM	--	Folder
Splatoon Hacks - Online Power Gauge Modifier	Jan 30, 2017, 7:10 PM	--	Folder
Gaugeriff	Jan 30, 2017, 3:05 PM	2 KB	rich text (RTF)
original.m4v	Jan 29, 2017, 10:37 PM	981.1 MB	MPEG-4 movie
Splatoon Hacks - Online Power Gauge Modifictomov	Jan 30, 2017, 4:43 PM	888.5 MB	QT movie
Splatoon Hacks - Online Private Battle in Inkopolis Plaza!	Jul 27, 2017, 12:18 PM	--	Folder
Splatoon Hacks - Turf War OverTime No Disconnect	May 28, 2017, 5:20 PM	--	Folder

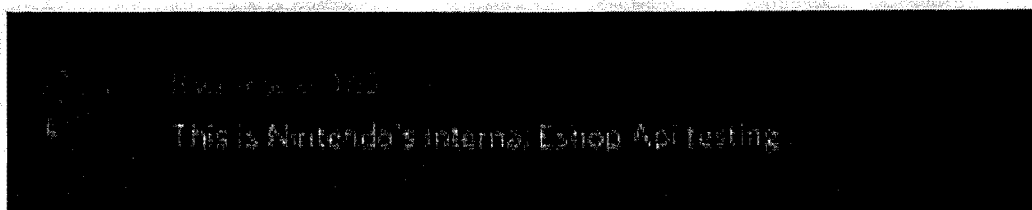
I also further noted that a Seagate drive (which I believe to be an external backup drive) was listed among the connected "Devices," which is consistent with the August 28 and September 3, 2018, Discord posts discussed above.

h. On February 4, 2019, Discord user "ryanrocks462" (HERNANDEZ) indicated that he needed to test a new piracy patch and posted multiple screenshots that he described as Nintendo internal servers, such as:

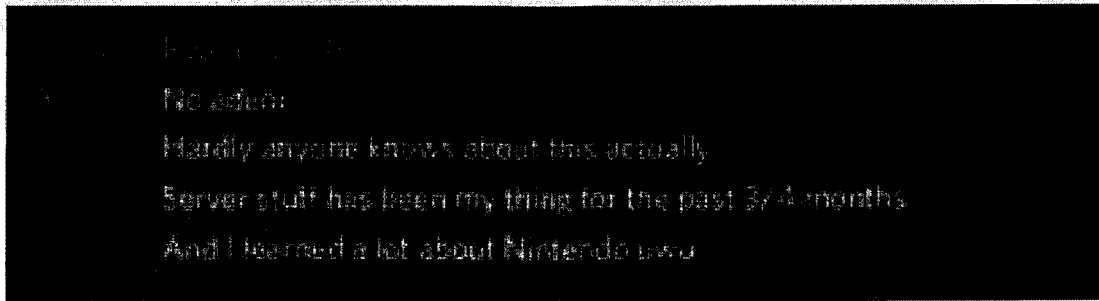
¹³ According to various online reference sites, "uwu" is Internet slang.



He further indicated that these images included Nintendo's internal eShop API testing server (which, as discussed above, is one of the server groups identified by Nintendo as having been compromised by HERNANDEZ):



User "ryanrocks462" (HERNANDEZ) further indicated that he had been working on Nintendo "Server stuff" for the past 3 to 4 months and had learned a lot about Nintendo:



(II) RYAN HERNANDEZ's Discord Posts

Regarding Prior Hacking Activity and FBI Contact

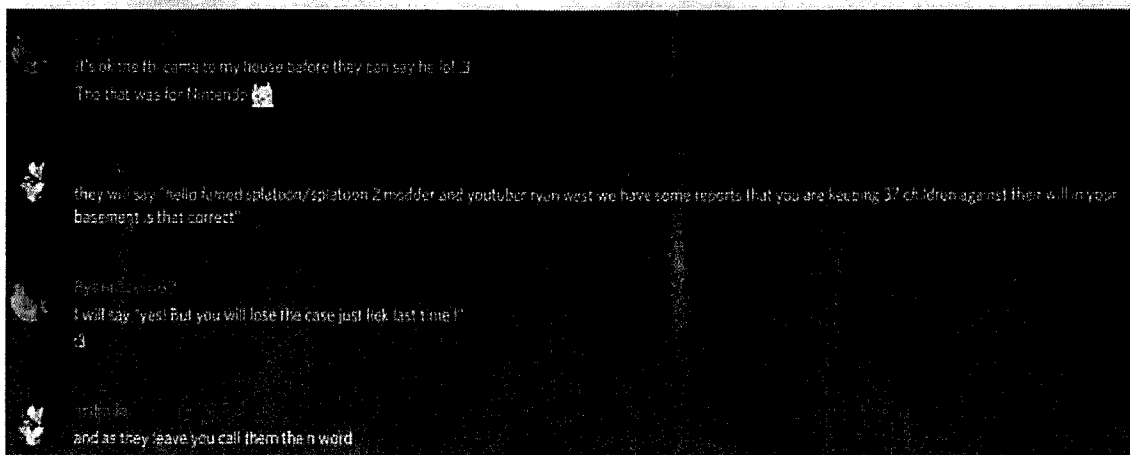
41. Discord user "ryanrocks462" (HERNANDEZ) also referenced his prior 2016-2017 hack of Nintendo's Developer Portal. For example:

a. On December 22, 2018, Discord user "ryanrocks462" (HERNANDEZ) engaged in communications with other users in which they discussed HERNANDEZ's prior hack of Nintendo's Developer Portal. Initially, "ryanrocks462" (HERNANDEZ) asked others for available storage, either on their computer or on a Google Drive, indicating he need "like 400GB" for a backup that possibly included "30,000 + links" and "pre-release stuff to." User "ryanrocks462" (HERNANDEZ) further suggested that the files related to "3ds/wiiu probably."

b. User "ryanrocks462" (HERNANDEZ) then told another user "U have to phish SDSG[,] Like anon did for me with the 16.7 sdk" and further explained the phishing methodology. As set forth in the tweet by user @ryanrocks462 (TWITTER ACCOUNT 1), above, HERNANDEZ thanked "anon" for helping with the leak of Switch SDK in October 2016. Based on my training and experience, and my involvement in this and the prior

investigation, I believe that HERNANDEZ's comments relate to his prior hack of Nintendo's Developer Portal, discussed above.

42. Discord user "ryanrocks462" (HERNANDEZ) also referenced his prior contact with FBI agents. Specifically, on November 24, 2018, Discord user "ryanrocks462" (HERNANDEZ) commented about how the FBI had previously come to his residence regarding Nintendo:



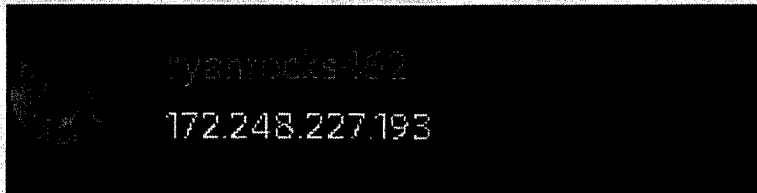
HERNANDEZ stated (likely humorously) that, if the FBI visited again, he would tell the FBI "you will lose the case just [like] last time !" I believe this is a reference to the fact that HERNANDEZ was not arrested or charged in relation to his prior Nintendo hack.

(III) HERNANDEZ's Discord Posts

Identifying His Home IP Address (HERNANDEZ HOME IP #1 and #2)

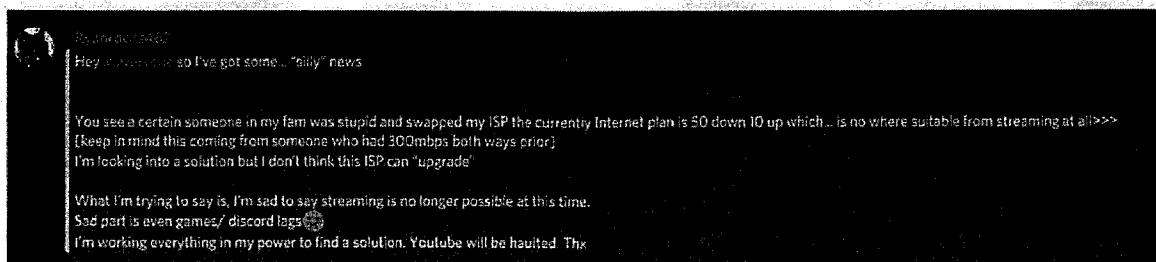
43. Discord user "ryanrocks462" (HERNANDEZ) also posted information confirming his IP addresses, namely, HERNANDEZ HOME IP #1 and HERNANDEZ HOME IP #2, used to intrude upon Nintendo's networks. For instance:

a. On about September 15, 2018, user "ryanrocks462" (HERNANDEZ) posted his IP address, HERNANDEZ HOME IP #1 (172.248.227.193):



As noted elsewhere, HERNANDEZ HOME IP #1 was identified by Nintendo as accessing its networks without authorization.

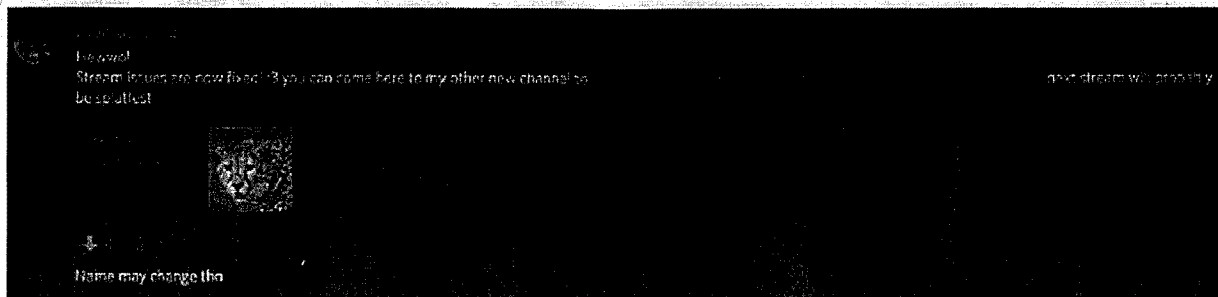
b. On about November 29, 2018, user "ryanrocks462" (HERNANDEZ) posted about his displeasure about a family member changing to a different Internet service provider with reduced download and upload speed, which caused him problems:



The post noted, among other things, that "someone in my fam was stupid and swapped my ISP." Based on the timing of the post, and my review of records obtained through FBI's investigation, discussed below, I believe HERNANDEZ's Discord post was reference to his father (Ruben) and his switch to AT&T as the new home Internet service provider (from Charter Communications, the provider of HERNANDEZ HOME IP #1) --- and in turn HERNANDEZ's switch to the new IP address 76.232.194.142

(HERNANDEZ HOME IP #2). As discussed below, according to records obtained from AT&T, the account associated with HERNANDEZ HOME IP #2 was established on November 21, 2018, for the **SUBJECT PREMISES**.

c. On December 3, 2018, Discord user "ryanrocks462" (HERNANDEZ) posted that the issues were resolved ("Stream issues are now fixed!") and included a link to his new YouTube channel, stating that his next stream would likely be "splatfest":



I recognize "splatfest" as a reference to the Nintendo Splatoon game.

ii. HERNANDEZ's Posts on Twitter

44. Nintendo also provided the FBI with screenshots and summaries of various posts (or "tweets") from two accounts believed to be used by HERNANDEZ, namely, User ID: 178776029, also known as username "@ryanrocks462" (TWITTER ACCOUNT 1) and User ID: 715225783, also known as username "@ryanrocks562" (TWITTER ACCOUNT 2). As discussed below, the FBI, through this and the prior investigation, confirmed that HERNANDEZ is the common user of both Twitter accounts.

(I) HERNANDEZ's Tweets About Nintendo and

Hacking-Related Activity

45. In tweets provided by Nintendo, HERNANDEZ referenced hacking activities on @ryanrocks462 (TWITTER ACCOUNT 1), such as the following:

a. As discussed above, in July 2017, Twitter user @ryanrocks462 (TWITTER ACCOUNT 1) appeared to take credit for the 2016-2017 hack of Nintendo's Developer Portal.

b. On September 29, 2017, Twitter user @ryanrocks462 (TWITTER ACCOUNT 1) tweeted about whether he should steal the Super Mario Odyssey demo unit "like I did with the 3ds carts before?" I believe this is a reference to HERNANDEZ's prior theft of Nintendo 3DS data as part of the above-described hack of the Nintendo Developer Portal.

c. On October 27, 2017, Twitter user @ryanrocks462 (TWITTER ACCOUNT 1) tweeted that he was quitting the hacking scene, specifically: "I Officially quit any 'haxing' scene. They no longer interest me. I may have not done much, but I managed to what I could. :P -Ryan^^".

d. On October 30, 2018, Twitter user @ryanrocks462 (TWITTER ACCOUNT 1) sent another tweet: "Honestly, I'm moving on from computer shit now. It was fun, but now a days it's just boring to me. Maybe I'll be a pilot that seems fun hehe". Shortly thereafter, Twitter user @ryanrocks462 (TWITTER ACCOUNT 1) followed up with a message: "I would like to announce due to some unexpected circumstances this account may 'possibly' be terminated by me soon."

e. Notably, FBI agents (including myself) contacted and interviewed HERNANDEZ at the **SUBJECT PREMISES** in Palmdale, California regarding the prior hack of Nintendo's Developer Portal on October 25, 2017 --- i.e., just days before these tweets about quitting "haxing" (hacking) and terminating his Twitter account. Accordingly, I believe that these messages are a direct reaction to law enforcement contact and interpret his statements as an acknowledgement by HERNANDEZ of his prior hacking ("haxing") activity. I also suspect that the realization of the FBI's awareness of and investigation into his illegal conduct is the "unexpected circumstances" that prompted HERNANDEZ to contemplate deleting TWITTER ACCOUNT 1.

f. HERNANDEZ did not ultimately delete or deactivate TWITTER ACCOUNT 1. Rather, on November 7, 2017, Twitter user @ryanrocks462 (TWITTER ACCOUNT 1) asked another Twitter user (@Govanify) for a recommendation for SSD encrypters and destroyers. This message suggests that HERNANDEZ was intending and/or attempting to encrypt and/or destroy stored data. Again, based on the timing, I suspect this relates to the prior hack of Nintendo and the recent law enforcement contact.

46. In September 2018, Twitter suspended @ryanrocks462 (TWITTER ACCOUNT 1). HERNANDEZ, using his other Twitter account @ryanrocks562 (TWITTER ACCOUNT 2), complained about the suspension of @ryanrocks462 (TWITTER ACCOUNT 1), and otherwise made clear that he is the user of both accounts:

Ryan ✨ 🛡️

@ryanrocks562

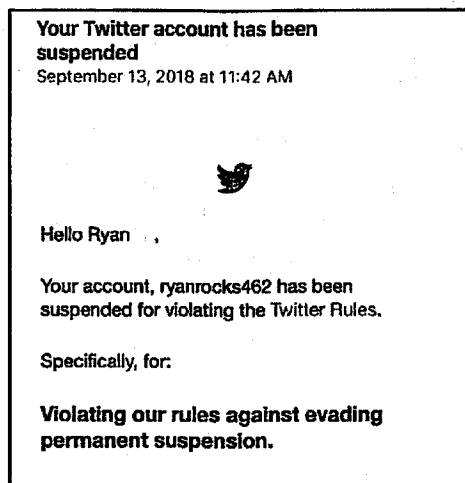
🇺🇸 I have a striving passion for illustration and animation. I walk alone. UDX HighSchool! You either hate me or you love me ٩(๏)٩ @Ryanrocks462 Acct Dead

📍 Somewhere w @HxVideoGameRev x3

🔗 twitter.com/ryanrocks462

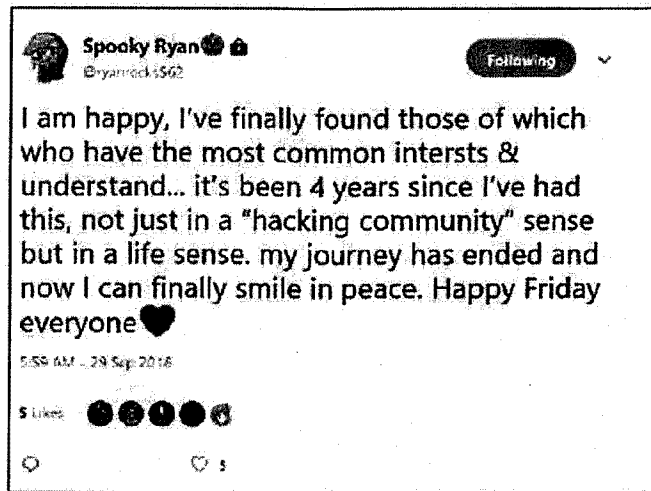
📅 Joined July 2012

47. Similarly, on September 17, 2018, Discord user "ryanrocks462" (HERNANDEZ) posted on HERNANDEZ DISCORD SERVER about Twitter account @ryanrocks462 (TWITTER ACCOUNT 1) having been suspended but that he was appealing, sharing the below image:



48. Twitter user @ryanrocks562 (TWITTER ACCOUNT 2) (HERNANDEZ) likewise has referenced hacking and made statements pertinent to the investigation. For instance,

a. On September 29, 2018, Twitter user @ryanrocks562 (TWITTER ACCOUNT 2) (HERNANDEZ) tweeted an expression of appreciation for having found a "hacking community":



I further note that the avatar for @ryanrocks562 (TWITTER ACCOUNT 2) appears to be the Link character from Nintendo's The Legend of Zelda franchise.

b. Also on about November 29, 2018, Twitter user @ryanrocks562 (TWITTER ACCOUNT 2) (HERNANDEZ) tweeted an image of the Spongebob Squarepants cartoon character wearing an FBI hat, with the message: "Hi @NintendoAmerica":



Notably, this tweet came only days after Discord user "ryanrocks462" (HERNANDEZ) mockingly discussed the prior contact by FBI agents regarding Nintendo, discussed above.

c. On December 9, 2018, Twitter user @ryanrocks562 (TWITTER ACCOUNT 2) announced that another Twitter user (@Cylints) had compromised his Epic games account and asked that user whether he/she used a "classic Phishing attack, or gather from another site database leak."

2. FBI's Current Investigation of HERNANDEZ's Nintendo Network Intrusion

49. As discussed herein, FBI is currently conducting an ongoing investigation of the recent 2018 intrusion of Nintendo's networks and has identified HERNANDEZ as the hacker. Below is merely a summary of investigative activity to date.

a. Confirmation of HERNANDEZ HOME IPs

50. Based on the review of records obtained through this investigation, it is apparent to me that HERNANDEZ was a user of HERNANDEZ HOME IP #1 (172.248.227.193) and HERNANDEZ HOME IP #2 (76.232.194.142). As discussed above, Nintendo also provided investigators with network logs and these IP addresses, which Nintendo gathered from its internal investigation of the hacking event. I have also reviewed network logs provided by Nintendo that record instances of unauthorized network access associated with the HERNANDEZ HOME IP #1 and #2.

51. Through this investigation, I have obtained records and information related to IP addresses used by HERNANDEZ at his Palmdale, California residence (**SUBJECT PREMISES**). I have

obtained and personally reviewed records obtained from the service providers, described below.

52. More specifically, I reviewed records obtained from Charter Communications, the service provider for HERNANDEZ HOME IP #1 (172.248.227.193).¹⁴ According to records obtained from Charter Communication in the prior investigation, as shown above, the account for HERNANDEZ HOME IP #1 was activated in December 2015 in the name of "Ruben Hernandez" (HERNANDEZ's father) at the **SUBJECT PREMISES**. According to updated records obtained in this investigation, the lease of HERNANDEZ HOME IP #1 (172.248.227.193) ended on November 29, 2018, as set forth below:

Lease			
Logger Status:	✓ Success		
IP Type:	IPv4 address	Original Lease Start:	6/7/2017 1:26:47 AM
IP Address:	172.248.227.193	Current Lease Start:	
MAC:	d405983403e4	Lease End:	11/29/2018 11:17:40 PM
CM MAC:	d405983403e2	Region:	Denver, CO

53. I also reviewed records obtained from AT&T, the service provider for HERNANDEZ HOME IP #2 (76.232.194.142). The account was established on November 21, 2018, registered to "Ruben Hernandez" at the **SUBJECT PREMISES**, as set forth below:

¹⁴ Investigators obtained subscriber records from Charter Communication as part of both the instant investigation and the prior investigation of the hack of Nintendo's Developer Portal.

> Subscriber Information	
Primary Contact Information Contact Name: RUBEN HERNANDEZ CBR: 001-501-2500 ALT CBR: 001-501-2502 Preferred Email: rherandez5630... Authenticated By: Passcode / QA <div>Flashes</div>	Account Information Account Id: [REDACTED] Account Name: RUBEN HERNANDEZ Member Id: [REDACTED] Established: 11/21/2018 Sub Type: Consumer Business Type: FTIN-SP Network Type: AT&T Billing: 2 Bill Cycle: Paper Bill Media: No AutoPay: English Bill Language:

54. As noted above, I also noted that this change in Internet service providers and IP address coincides with HERNANDEZ's posts on Discord, further confirming that HERNANDEZ was a user of HERNANDEZ HOME IP #1 (172.248.227.193) and HERNANDEZ HOME IP #2 (76.232.194.142). Both these IP addresses have been identified as having been used to access Nintendo's networks without authorization.

b. HERNANDEZ's Use of Yahoo Accounts

55. Based on the review of records related to numerous accounts, it is apparent to me that HERNANDEZ frequently has used his Yahoo accounts, namely, ryanrocks462@yahoo.com (YAHOO ACCOUNT 1), ryanrocks562@yahoo.com (YAHOO ACCOUNT 2), and ryanrocks463@yahoo.com (YAHOO ACCOUNT 3), particularly to register other email and social media accounts.

56. I obtained and reviewed records from Oath (Yahoo) for each account. Each of these Yahoo accounts is registered using HERNANDEZ's known alias "Ryan West."

a. According to records obtained from Oath, account ryanrocks462@yahoo.com (YAHOO ACCOUNT 1) was registered in 2009,

and is in the name "Mr Ryan West" with an alternative email address of ryanrocks463@yahoo.com (YAHOO ACCOUNT 3):

Login Name:	ryanrocks462
GUID:	RVPGZ7RYWQY4GFOB2J5FUHJAA
Properties Used:	Answers Flickr Mail
Yahoo Mail Name:	ryanrocks462@yahoo.com
Alternate Communication Channels:	ryanrocks463@yahoo.com <i>Verified</i> 1 6613613779 <i>Verified</i>
Registration IP address:	75.40.64.184
Account Created (reg):	Wed Oct 14 01:02:22 2009 GMT
Other Identities:	ryanrocks462 (Yahoo! Mail)
Full Name	Mr Ryan West

b. Account ryanrocks562@yahoo.com (YAHOO ACCOUNT 2) was registered in 2011, in the name "Ryan West" with an alternative email address of ryanrocks462@yahoo.com (YAHOO ACCOUNT 1):

Login Name:	ryanrocks562
GUID:	V2ZEQBT6CNEM2DHIS5SSOB4SE
Properties Used:	Mail Groups
Yahoo Mail Name:	ryanrocks562@yahoo.com
Alternate Communication Channels:	ryanrocks462@yahoo.com <i>Verified</i> 1 6613613779 <i>Verified</i>
Registration IP address:	184.72.15.185
Account Created (reg):	Tue May 17 06:40:07 2011 GMT
Other Identities:	ryanrocks562 (Yahoo! Mail)
Full Name	Ryan West

c. Account ryanrocks463@yahoo.com (YAHOO ACCOUNT 3) was registered in 2012, in the name "Ryan West":

Login Name:	ryanrocks463
GUID:	QJ5CXVGAPVUOO6WSNGOHPGPR6A
Properties Used:	Mail
Yahoo Mail Name:	ryanrocks463@yahoo.com
Alternate Communication Channels:	1 6613613779 <i>Verified</i>
Registration IP address:	75.22.49.170
Account Created (reg):	Sat Apr 14 04:33:17 2012 GMT
Other Identities:	ryanrocks463 (Yahoo! Mail)
Full Name	Ryan West

57. According to logs provided by Oath, as of December 11, 2018 (the end date of Oath's production range), each of these "ryanrocks" Yahoo accounts had been accessed on December 11, 2018, which leads investigators to believe that the accounts remain active. Moreover, each account was accessed from HERNANDEZ HOME IP #2 (76.232.194.142), associated with the **SUBJECT PREMISES**, as recently as December 9, 2018.

58. HERNANDEZ's three Yahoo accounts are all associated with the same phone number, 661-361-3779.

59. According to records obtained from AT&T, the service provider, the phone number is registered to Ruben Hernandez (HERNANDEZ's father) at the **SUBJECT PREMISES**:

USER INFORMATION

MSISDN: (661) 361-3779
 IMSI: 310410054528016
 MSISDN Active: 03/10/2013 - Current
 Name: RUBEN F HERNANDEZ
 User Address: 40520 ASTER PL, PALMDALE, CA 93551
 Service Start Date: 03/10/2013
 Dealer Info: K8FL0 K8FL0 K8FL0
 Payment Type: Postpaid
 Contact Name: RUBEN F HERNANDEZ
 Contact Home Phone:
 Contact Work Phone:
 Contact Home Email: Rhernandez5630@gmail.com
 Contact Work Email:

The number was activated in March 2013 and remained active as of the production date (approximately February 23, 2019).

c. Confirmation of HERNANDEZ's Discord Account

60. Based on the review of records obtained through this investigation, it is apparent to me that HERNANDEZ was the user of Discord account "ryanrocks462" and the operator of "Ryan's Underground Hangout" (HERNANDEZ DISCORD SERVER).

61. According to records obtained from Discord, which I reviewed, account "ryanrocks462" was registered on May 31, 2018, from HERNANDEZ HOME IP #1 (172.248.227.193), using email ryanrocks463@yahoo.com (YAHOO ACCOUNT 3):

User ID:	451537312900317201
Username:	Ryanrocks462#8138
Email:	ryanrocks463@yahoo.com
Registration Time (UTC):	2018-05-31 00:08:05
Registration IP:	172.248.227.193

62. Additionally, Discord IP log records confirmed that HERNANDEZ's account was accessed regularly from HERNANDEZ HOME IP #1 (172.248.227.193), i.e., from the **SUBJECT PREMISES** and the same IP address used to access Nintendo's network, between at least August 18, 2018 (the first date of the logs provided) until November 28, 2018. Thereafter, Discord account "ryanrocks462" (HERNANDEZ) was regularly accessed through HERNANDEZ HOME IP #2 (76.232.194.142).

63. As noted above, according to records obtained from AT&T, the account associated with HERNANDEZ HOME IP #2 (76.232.194.142) was established on November 21, 2018,

registered to "Ruben Hernandez," at the **SUBJECT PREMISES**.

Moreover, as noted above, on about November 29, 2018, Discord user "ryanrocks462" (HERNANDEZ) posted about his displeasure about a family member changing to a different Internet service provider with reduced download and upload speed.

d. Confirmation of HERNANDEZ's Twitter Accounts

64. Based on the review of records obtained through this investigation, it is apparent to me that RYAN HERNANDEZ was the user of account @ryanrocks462 (TWITTER ACCOUNT 1) and account @ryanrocks562 (TWITTER ACCOUNT 2). I also obtained a search warrant for these Twitter accounts, and my review of the return material confirms the Twitter-related information provided by Nintendo, discussed above.

65. I obtained and reviewed records from Twitter for each account. According to records obtained from Twitter, account @ryanrocks462 (TWITTER ACCOUNT 1) was created in 2010, and is associated with email address ryanrocks462@yahoo.com (YAHOO ACCOUNT 1):

```
-----BEGIN PGP SIGNED MESSAGE-----  
Hash: SHA512  
  
account_id: 178776029  
created_at: 2010-08-15 17:23:46 +0000  
updated_at: 2018-09-13 20:01:18 +0000  
email: ryanrocks462@yahoo.com  
created_via: web  
screen_name: ryanrocks462  
time_zone: Pacific Time (US & Canada)  
*****
```

Moreover, according to IP logs provided by Twitter, TWITTER ACCOUNT 1 was repeatedly accessed through the **SUBJECT PREMISES**

using HERNANDEZ HOME IP #1 (172.248.227.193) through at least October 26, 2018.¹⁵ Below is an example of a TWITTER ACCOUNT 1 login on October 26, 2018:

```
account_id: 178776029
created_at: 2018-10-26 23:29:48 +0000
last_login_ip: 172.248.227.193
*****
```

66. According to records obtained from Twitter, account @ryanrocks562 (TWITTER ACCOUNT 2) was created in 2012, and is associated with email address ryanrocks562@yahoo.com (YAHOO ACCOUNT 2):

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

account_id: 715225783
created_at: 2012-07-25 01:11:08 +0000
updated_at: 2019-02-15 14:50:15 +0000
email: ryanrocks562@yahoo.com
created_via: m5
screen_name: ryanrocks562
time_zone:
*****
```

Moreover, according to IP logs provided by Twitter, TWITTER ACCOUNT 2 was repeatedly accessed through the **SUBJECT PREMISES** using HERNANDEZ HOME IP #2 (76.232.194.142) through at least

¹⁵ Investigators have Twitter IP log information for TWITTER ACCOUNT 1 from September 20, 2018, through about November 19, 2018, the date records were received from Twitter. This predates the change in Internet service providers to AT&T and HERNANDEZ HOME IP #2 (76.232.194.142).

February 14, 2019.¹⁶ Below is an example of a TWITTER ACCOUNT 2 login on February 14, 2019:

```
account_id: 715225783
created_at: 2019-02-14 22:08:36 +0000
last_login_ip: 76.232.194.142
*****
```

e. Search Warrants of HERNANDEZ's Accounts

68. On about February 21, 2019, the Honorable Mary Alice Theiler, Magistrate Judge for the Western District of Washington, authorized search warrants on various accounts used by RYAN HERNANDEZ at Discord, Twitter, Apple, and Google, including Twitter accounts "@ryanrocks462" (TWITTER ACCOUNT 1) and "@ryanrocks562" (TWITTER ACCOUNT 2) and the HERNANDEZ DISCORD SERVER.

69. Responsive material received to date from the various providers are in the process of being reviewed and analyzed by investigators, including myself.

70. Records provided by Twitter for accounts "@ryanrocks462" (TWITTER ACCOUNT 1) and "@ryanrocks562" (TWITTER ACCOUNT 2) also included evidence of criminal activity, including many of the Twitter posts described above. For instance, I immediately noted the series of tweets from TWITTER ACCOUNT 1 in October 2017, where HERNANDEZ stated, "I Officially Quit any \"haxing\" scene,. . .," described above, which followed FBI's interview of him at the **SUBJECT PREMISES**.


¹⁶ Investigators have Twitter IP log information for TWITTER ACCOUNT 2 from January 4, 2019, through February 14, 2019, the date records were received from Twitter.

71. In addition, HERNANDEZ's Twitter accounts contained additional evidence of his involvement in the various hacking ventures described herein. For instance,


a. The Twitter records included a photograph related to HERNANDEZ's agreement with Nintendo in about September 2016, discussed above, in which he agreed to cease hacking activities and cease use of Nintendo's developer sites and confidential and proprietary information.

b. The Twitter records also included a screenshot of what appears to be confidential files related to the Nintendo 3DS gaming console.


c. The Twitter records also included a screenshot of what I believe to be the initial phishing communication used to compromise the Nintendo Developer Portal in October 2016, also discussed above:














Nickname (Required)  Brenden Gibbs





Subject (Required) MultiThreading issue: Fatal error

Development Environment (Required)  CTR-SDK_11.5.1

Priority High

Comment (Required) 

B I U S             

14px     Source

Hello,

I appear to be having an issue with my title. Ever since upgrading to CTR_SDK 11.5.1 it appears that when I do advanced multi-threading the system just crashes. The source code would probably be more useful to you, so here is a link with the source and a picture of the error.

<http://devshareportal.byeethost18.com/share-8b45d28a2d/>

Can someone shed some light into what is causing this issue?

Regards,
Brenden

The message purports to originate from a user named "Brenden Gibbs," requested customer support related to an issue relating to SDK, and contained a link to an external site. This message is consistent with Nintendo's description of the 2016-2017 phishing compromise. Furthermore, as described above, this message is consistent with HERNANDEZ's own description of the prior hack of Nintendo's Developer Portal on both Discord and Twitter.

72. Google has provided limited records and information related to HERNANDEZ's Google account, ryanrocks562@gmail.com (hereinafter, "GOOGLE ACCOUNT 1"). I did note that HERNANDEZ's Internet browsing history logged a visit to <https://pastebin.com/u/SciressM> in November 2017. This site contains a trove of Nintendo-related files. I also noted searches for blogs related to "3ds," which I believe to be reference to the Nintendo 3DS console, in 2016.

73. On April 18, 2019, investigators received responsive records and information from Discord related to HERNANDEZ's account (username "ryanrocks462") and his "server," "Ryan's Underground Hangout" (HERNANDEZ DISCORD SERVER), which I am in the process of reviewing.

74. Through my review to date, I have encountered evidence of criminal activity, including many of the Discord posts described above provided by Nintendo, among others. Below are summaries of certain chats, as examples:

a. On June 25, 2018, HERNANDEZ and another Discord user discussed manipulating authentication certificates in an effort to break into Nintendo's CDN and download content.

b. On August 14, 2018, HERNANDEZ explained to another Discord user how to successfully manipulate Nintendo device tokens and authentication certificate files.

c. On December 28, 2018, HERNANDEZ lamented that "I'm still trying to work making a php script to steal session cookies ~~I need the newest switch sdk~~"

Based on my training and experience and involvement in this investigation, I know that these comments refer to hacking techniques and specifically techniques utilized in the intrusion activity under investigation.

75. Also included in the Discord records and information reviewed to date, I have noted references to prior hacking activity targeting Nintendo. For instance,

a. On June 6, 2018, HERNANDEZ commented about gaining access to insider knowledge at the E3 conference by lying and claiming he was with the press. The Electronic Entertainment Expo, commonly referred to as "E3," is a trade event for the video game industry. The event is used by many developers, publishers, and hardware and accessory manufacturers (including Nintendo) to introduce and advertise upcoming games and game-related merchandise to retailers and members of the press. According to information provided by Nintendo, HERNANDEZ has attended E3 conferences in the past and, in 2016, was caught

attempting to gain access to a pre-release Zelda game at the Nintendo exhibition.

b. In the same conversation on June 6, 2018, HERNANDEZ said he spends his time with "YouTube + haxing ppl + organization with haxing ppl + reversing splatty 2 + making time for friends + dealing with side tasks such as getting pics for a preservation dumping project of Nintendo titles."

c. On September 26, 2018, HERNANDEZ detailed his prior hack of Nintendo's Developer Portal, stating "And add my own IP addesss for he server whitelist. Just steals a session from admin on dev portal. That's how the 2016 sdk leaked. With me and anon."

d. In the same conversation above, HERNANDEZ stated that he "Just gotta steal a session cookie again" so that he can return to the "Good ol days" where "internal servers had games 6 months early + Internal tools and retail devmenu."

e. More recently, in January 2019, HERNANDEZ commented that he is "very happy" because "Nintendo believed my lies and now I have switch access."

f. On April 12, 2019, HERNANDEZ asked another Discord user for permanent Google Drive space that he could host 17.5 GB of Nintendo CDN content that "includes, all of wii, dsi, 3ds, wiiu, and switch." As discussed above, I recognize this comment to reference Nintendo's various game consoles.

f. **HERNANDEZ's Use of Amazon Accounts**

76. Through this investigation, investigators further obtained records from Amazon for marketplace accounts associated

with ryanrocks562@yahoo.com (YAHOO ACCOUNT 2) and ryanrocks463@yahoo.com (YAHOO ACCOUNT 3). According to Amazon records, the name on the account associated with YAHOO ACCOUNT 2 is "ryan" with a primary address of RYAN HERNANDEZ, 40520 Aster Pl, Palmdale, CA 93551 (**SUBJECT PREMISES**).

77. Notably, HERNANDEZ's Amazon account records also included among the numerous registered payment accounts a credit card under the name of "Brendan" associated with the **SUBJECT PREMISES**, created on June 7, 2017. Further, according to the retail order log, on about June 7, 2017, the same account attempted, but cancelled, an order for "eCash - Nintendo eShop Gift Card \$70 - Switch / Wii U / 3DS [Digital Code]" using the credit card associated with name "Brendan." The order was made using HERNANDEZ HOME IP #1 (172.248.227.193) at the **SUBJECT PREMISES**. "Brendan" is similar to the name "Brenden Gibbs" used in the suspected phishing message, above.

78. Also notable, according to the log of retail orders, on about May 13, 2017, HERNANDEZ's Amazon account associated with YAHOO ACCOUNT 2 purchased a "Seagate Backup Plus Hub 8TB External Desktop Hard Drive Storage (STEL8000100)" for \$179.99, which was shipped to the **SUBJECT PREMISES**. The order also was made using HERNANDEZ HOME IP #1 (172.248.227.193) at the **SUBJECT PREMISES**. As discussed above, reference to a Seagate backup hard drive is visible on HERNANDEZ's various media posts. Moreover, investigators believe that the external drive was used to facilitate the scheme and currently is located at the **SUBJECT PREMISES**.

79. HERNANDEZ's account associated with YAHOO ACCOUNT 3 is "ryan" with a primary address of RYAN HERNANDEZ, 40520 Aster Pl, Palmdale, CA 93551 (**SUBJECT PREMISES**) and a registered credit card belonging to Ruben Hernandez at the **SUBJECT PREMISES**. According to IP logs, from November 23, 2017 (account creation) to November 22, 2018, the account had multiple log-ins from HERNANDEZ's IP address at the **SUBJECT PREMISES** (172.248.227.193).

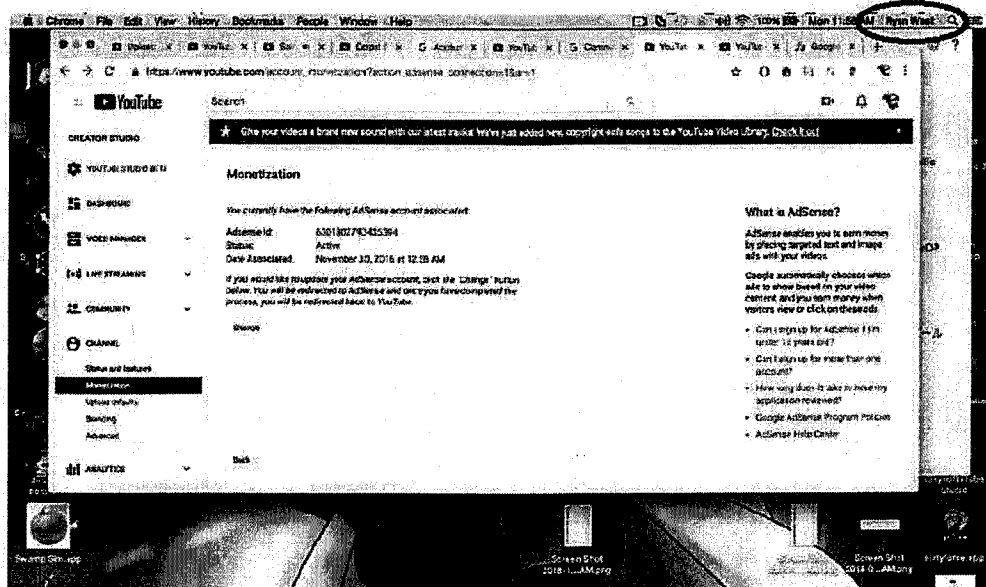
g. Additional Confirmation of HERNANDEZ's Use of Alias "Ryan West"

80. As noted herein, RYAN HERNANDEZ used aliases, including "Ryan West," in conjunction with various online accounts.

81. By way of further example, HERNANDEZ maintained a Facebook account under the username "ryan.west.462" (hereinafter, "FACEBOOK ACCOUNT"). I have reviewed publicly accessible portion of the FACEBOOK ACCOUNT and believe it to belong to HERNANDEZ. I obtained and reviewed subscriber records for FACEBOOK ACCOUNT. The account was registered in May 2011 under the name Ryan West, using ryanrocks562@yahoo.com (YAHOO ACCOUNT 2). The associated payment information included a Visa credit card ending in -8048, and an American Express card ending in -1723, both in the name of RYAN HERNANDEZ, as well as a PayPal account associated with email ryanrocks562@yahoo.com (YAHOO ACCOUNT 2).

82. Furthermore, as discussed above, HERNANDEZ (Discord user "ryanrocks462") posted various screenshots of his computer

desktop on Discord, as indicated in material provided by Nintendo. In many such screenshots, the username of "Ryan West" appears in the desktop toolbar, as set forth in the example below:



h. Recent Evidence of Hacking Activity

83. On June 17, 2019, I participated in a call with representatives of Nintendo, who advised me of the following:

a. HERNANDEZ has continued to access its networks and conduct malicious activity. For example, according to Nintendo, on May 11, 2019, HERNANDEZ attempted thousands of logins to a restricted Nintendo FTP server using various Nintendo credentials. On the same date, May 11, 2019, HERNANDEZ successfully downloaded over 145,000 "objects" (which Nintendo described as digital items similar to files) from non-public servers hosting the staging environment for Nintendo games.

b. HERNANDEZ attended the 2019 E3 conference, held in Los Angeles on June 11-13, 2019. Based on past concerns, Nintendo had circulated HERNANDEZ's photograph to its personnel. HERNANDEZ visited the Nintendo booth and engaged the Nintendo representative on multiple occasions. During one such conversation, HERNANDEZ asked various probing questions about technical aspects of the Switch console, which the representative found concerning.

i. Additional Confirmation of HERNANDEZ's Residence at the SUBJECT PREMISES

84. Based on information gathered through the investigation, I believe that RYAN HERNANDEZ continues to reside at the **SUBJECT PREMISES**. I also believe evidence and instrumentalities of criminal activity, including various devices, such as computers, phones, Nintendo consoles, and other devices, used to facilitate his criminal offenses are located at the **SUBJECT PREMISES**.

85. According to records obtained from the California Department of Motor Vehicles in February 2019, HERNANDEZ, born in 1999, listed a residential address of 40520 Aster Pl, Palmdale, CA 93551 (**SUBJECT PREMISES**). HERNANDEZ applied for the license on May 10, 2017, which remains valid until January 2023.

86. On March 13, 2019, FBI SA David Garcia conducted surveillance at 40520 Aster Place, Palmdale, CA 93551 (**SUBJECT PREMISES**). SA Garcia took photographs and noted a description of the **SUBJECT PREMISES**. I reviewed the photographs and

recognized the **SUBJECT PREMISES** as HERNANDEZ's residence because, as described above, I interviewed defendant with his parents at the **SUBJECT PREMISES** in October 2017.

87. In addition, SA Garcia observed three vehicles at the **SUBJECT PREMISES**, as follows:

a. A 2015 black Honda Accord sedan bearing California license plate number 7[XXX]082 was observed parked directly in front of the residence. A check of the California Department of Motor Vehicle (DMV) database revealed that the registered owner of the vehicle returns to a Ruben Franco Hernandez with a listed address of 40520 Aster Place, Palmdale, California 93551 (**SUBJECT PREMISES**). The registration is currently valid from 9/22/2018 to 9/22/2019.

b. A 2016 white Ford F-150 truck bearing California license plate number 1[XXX]3E2 was observed parked inside the garage of the residence. A check of the California DMV database revealed that the registered owner of the vehicle returns to a Sheila Marlynn Hernandez with a listed address of 40520 Aster Place, Palmdale, California 93551 (**SUBJECT PREMISES**). The registration is currently valid from 2/28/2019 to 2/28/2020.

c. A 2015 white Lincoln sedan bearing California license plate number 7[XXX]619 was observed parked inside the garage of the residence. A check of the California DMV database revealed that the registered owner of the vehicle returns to a Sheila Marlynn Hernandez with a listed address of 40520 Aster Place, Palmdale, California 93551 (**SUBJECT PREMISES**). The registration is currently valid from 3/8/2019 to 3/8/2020.

88. Based on my participation in the investigation of RYAN HERNANDEZ, I know Ruben and Sheila Hernandez to be HERNANDEZ's parents, who also reside at the **SUBJECT PREMISES** with HERNANDEZ.

89. As mentioned above, investigators (including myself) contacted and interviewed RYAN HERNANDEZ in October 2017 at the **SUBJECT PREMISES**. That interview, among other things, confirmed he resided at that residence with his parents.

90. As discussed above, HERNANDEZ also has frequently accessed his various accounts through the IP addresses associated with the **SUBJECT PREMISES**.

91. Based on my training and experience, and my involvement in this and the prior investigation, I believe that RYAN HERNANDEZ currently resides at the **SUBJECT PREMISES** and has resided at the **SUBJECT PREMISES** since at least 2015. I further believed that evidence, fruits, and instrumentalities of the criminal offenses under investigation are located at the **SUBJECT PREMISES**.

i. **Additional Information Regarding Devices and Other Evidence at the SUBJECT PREMISES and HERNANDEZ's Use of HERNANDEZ HOME IPs**

92. The records and information gathered through this investigation included tweets by the user of @ryanrocks562 (TWITTER ACCOUNT 2) and @ryanrocks462 (TWITTER ACCOUNT 1), which I know to be a social media service accessible on a variety of electronic devices, including phones, tablets, as well as computers. I also know that people typically retain such items and devices in their residences and/or on their person.

93. HERNANDEZ's online activity also included posts by Discord user "ryanrocks462" (HERNANDEZ) that included screenshots and photographs that appear to have originated from both a computer and a phone. I also know based on my review of records provided by Apple that HERNANDEZ appears to periodically update his iPhone. I believe that such devices, among other items of interest, will be located at the **SUBJECT RESIDENCE**.

94. Through various posts, HERNANDEZ also discussed owning various Nintendo products and consoles. He further described attempted modifications to his personal Nintendo devices. For instance,

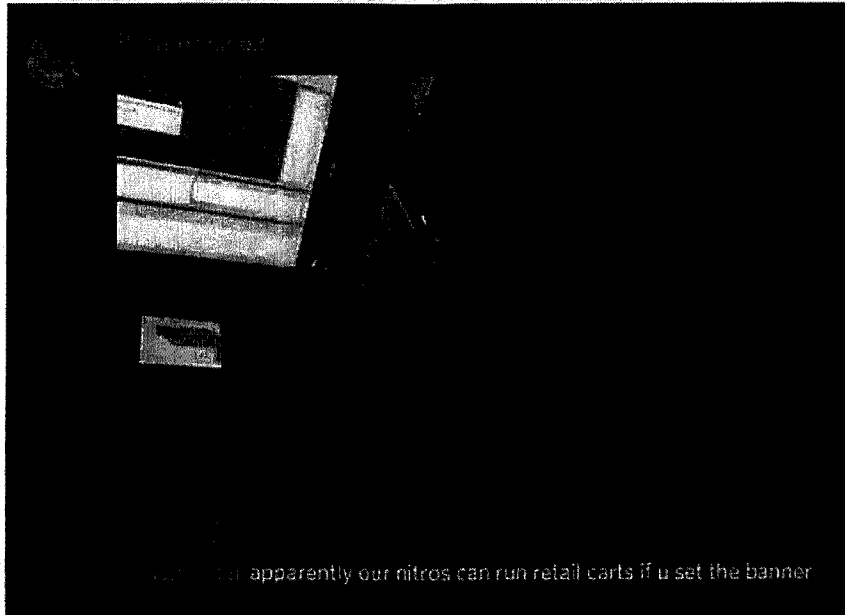
a. In October 2017, Discord user "ryanrocks462" (HERNANDEZ) posted photographs of his attempt to modify a Nintendo Wii-U console.

b. In April 2018, Twitter user @ryanrocks462 (HERNANDEZ) posted a video of a Nintendo Switch displaying a SEGA logo on its screen. I understand this to suggest that HERNANDEZ has somehow modified the code of his Nintendo console to expand its usage to operate games and code of other manufacturers and developers.

c. On about September 26, 2018, Discord user "ryanrocks462" (HERNANDEZ) posted a photograph of a Nintendo Development Kit.

d. On about December 3, 2018, Discord user "ryanrocks462" (HERNANDEZ) posted a photograph of what appears to be a Nintendo 3DS console and a Nintendo development unit connected to a laptop. HERNANDEZ included a message to user

"thomasnet" that "apparently our nitros can run retail carts if u set the banner."



95. Based on my training and experience, I recognize Apple devices, both a laptop and iPhone, and Apple (Mac) user interface in various images posted by HERNANDEZ in the accounts discussed above.

96. According to records obtained from Apple, it appears that RYAN HERNANDEZ has purchased and/or utilized numerous iPhones since 2013, including an iPhone 7 in 2016 and an iPhone X in November 2017:

purchase date	product description	customer name	contact name	dsid	apple login id
2009-04-05 00:00:00	IPOD TOUCH (2ND GEN) 8GB-USA	ryan hernandez		1092155705	ryanrock452@yahoo.com
2013-03-10 00:00:00	SVC IPHONE 5, GSM, 16GB, BLACK, CI	Ruben Hernandez		1710515926	ryanrock463@yahoo.com
2013-03-10 00:00:00	IPHONE 5 BLACK 16GB AT&T-USA	Ruben Hernandez		1710515926	ryanrock463@yahoo.com
2013-03-10 00:00:00	SVC IPHONE 5, GSM, 16GB, BLACK, CI	Ruben Hernandez		1710515926	ryanrock463@yahoo.com
2013-03-26 00:00:00	IPOD SHUFFLE 2GB SILVER-USA	ryan hernandez	ryan hernandez	1092155705	ryanrock462@yahoo.com
2013-10-25 00:00:00	IPHONE 5S GOLD 32GB-USA	Ruben Hernandez	Ruben Hernandez	1710515926	ryanrock463@yahoo.com
2014-07-05 00:00:00	MBP 15.4/2.9GHZ/16GB/512GB FU	Ruben Hernandez		1710515926	ryanrock463@yahoo.com
2014-11-12 00:00:00	IPHONE 5 GOLD 64GB AT&T-USA	Ruben Hernandez		1710515926	ryanrock463@yahoo.com
2014-12-30 00:00:00	IPHONE 5S SPACE GRAY 64GB AT&T	Ruben Hernandez		1710515926	ryanrock463@yahoo.com
2015-09-30 00:00:00	IPHONE 5S GOLD 128GB AT&T-USA	Ruben Hernandez		1710515926	ryanrock463@yahoo.com
2016-09-12 00:00:00	IPHONE 7 JET BLACK 256GB AT&T	Ruben Hernandez		1710515926	ryanrock463@yahoo.com
2016-09-13 00:00:00	SVC IPHONE 7, GSM, 256GB, JBLK, CI	Ruben Hernandez		1710515926	ryanrock463@yahoo.com
2017-11-21 00:00:00	IPHONE X SPACE GRAY 256GB AT&T	Ruben Hernandez		1710515926	ryanrock463@yahoo.com

Each iPhone is listed in the customer name of HERNANDEZ's father (Ruben) and associated with one of HERNANDEZ's Yahoo email addresses, namely, ryanrocks463@yahoo.com (YAHOO ACCOUNT 3), and the **SUBJECT PREMISES**.

97. From records obtained from Apple, investigators identified three Apple iCloud accounts associated with HERNANDEZ; but, according to activity logs, only one, Apple ID 1710515926, associated with ryanrocks462@icloud.com (hereinafter, "iCLOUD ACCOUNT"), appears in use.¹⁷ HERNANDEZ's iCLOUD ACCOUNT is associated with ryanrocks463@yahoo.com (YAHOO ACCOUNT 3) and is registered in the name of Ruben Hernandez (HERNANDEZ's father) at the **SUBJECT PREMISES** in Palmdale, California. The iCLOUD ACCOUNT is linked to iTunes and Gamecenter activity exclusively in the name of RYAN HERNANDEZ of the **SUBJECT PREMISES**.

98. The iCloud logs obtained from Apple for the iCLOUD ACCOUNT suggest almost daily, account activity during the period for which records were provided, from November 22, 2018 to December 11, 2018. Further, the vast majority of the log activity for the iCLOUD ACCOUNT is associated with HERNANDEZ HOME IP #1 (172.248.227.193) until November 27, 2018, and HERNANDEZ HOME IP #2 (76.232.194.142) thereafter. A sample excerpt from a portion of the iCLOUD ACCOUNT activity on December 4, 2018 is below:

¹⁷ The other two iCloud accounts (Apple ID 1092155705 and 1706835673) are associated with emails ryanrocks462@yahoo.com (YAHOO ACCOUNT 1) and ryanrocks562@yahoo.com (YAHOO ACCOUNT 2), respectively, and in the name RYAN HERNANDEZ.

1710515926	Service=iCLOUDDRIVE	timestamp="Tue Dec 04 17:41:22.103 PST 2018"	Device Type and OS="MacBookPro11,3" "OSX;10.10.x"	76.232.194.142
1710515926	Service=iCLOUDDRIVE	timestamp="Tue Dec 04 17:41:22.100 PST 2018"	Device Type and OS=	76.232.194.142
1710515926	Service=SAFARIBROWSINGHISTORY	timestamp="Tue Dec 04 17:41:21.793 PST 2018"	Device Type and OS="MacBookPro11,3" "OSX;10.10.x"	76.232.194.142
1710515926	Service=SAFARIBROWSINGHISTORY	timestamp="Tue Dec 04 17:41:21.786 PST 2018"	Device Type and OS=	76.232.194.142
1710515926	Service=iCLOUDDRIVE	timestamp="Tue Dec 04 17:41:21.358 PST 2018"	Device Type and OS="MacBookPro11,3" "OSX;10.10.x"	76.232.194.142
1710515926	Service=iCLOUDDRIVE	timestamp="Tue Dec 04 17:41:21.353 PST 2018"	Device Type and OS=	76.232.194.142
1710515926	Service=SAFARIBROWSINGHISTORY	timestamp="Tue Dec 04 17:41:20.335 PST 2018"	Device Type and OS="MacBookPro11,3" "OSX;10.10.x"	76.232.194.142
1710515926	Service=CONTACTS	timestamp="Tue Dec 04 17:41:19.101 PST 2018"	Device Type and OS=	76.232.194.142
1710515926	Service=SAFARIBROWSINGHISTORY	timestamp="Tue Dec 04 17:41:18.964 PST 2018"	Device Type and OS="MacBookPro11,3" "OSX;10.10.x"	76.232.194.142
1710515926	Service=SAFARIBROWSINGHISTORY	timestamp="Tue Dec 04 17:41:18.962 PST 2018"	Device Type and OS=	76.232.194.142
1710515926	Service=CONTACTS	timestamp="Tue Dec 04 17:41:18.776 PST 2018"	Device Type and OS=	76.232.194.142
1710515926	Service=CONTACTS	timestamp="Tue Dec 04 17:41:18.651 PST 2018"	Device Type and OS=	76.232.194.142

99. Based on my review of evidence, including the iCloud log activity and his various account activity, I know that HERNANDEZ was active on linked devices using HERNANDEZ HOME IP #1 and HERNANDEZ HOME IP #2 of the **SUBJECT PREMISES** at the time he was engaged in the threat activity under investigation. I further believe that those devices are located at the **SUBJECT PREMISES** and contain evidence of, and served as instrumentalities of, the criminal conduct under investigation.

100. From various screenshots posted by RYAN HERNANDEZ, it appears that HERNANDEZ also used Google Chrome and various Google services. For instance, according to records obtained from Google, HERNANDEZ's Google account associated with email ryanrocks562@gmail.com (hereinafter, "GOOGLE ACCOUNT 1") is associated with numerous Google products and services, including email, Google Chrome, Google Drive and YouTube, as set forth in the subscriber information below:

GOOGLE SUBSCRIBER INFORMATION

Name: Ryan West

e-Mail: ryanrocks562@gmail.com

Services: Android, Blogger, Chromeos Login, Glass, Gmail, Google
AdSense, Google AdWords, Google Calendar, Google Chrome Sync,
Google Docs, Google Drive, Google Hangouts, Google Maps Engine,
Google My Maps, Google Payments, Google Photos, Google Play,
Google Play Music, Google Sites, Google URL Shortener, Google
Voice, Google+, Has Google Profile, Has Madison Account, Has
Plusone, Location History, Web & App Activity, YouTube, YouTube
CMS, iGoogle

Recovery e-Mail: ryanrocks462@yahoo.com

Created on: 2010/08/04-22:33:32-UTC

Terms of Service IP: 98.148.168.104, on 2010/08/04-22:33:32-UTC

SMS: +16613613779 [US]

Alternate e-Mail(s): ryanrocks462@yahoo.com

Google Account ID: 279578011651

Last Logins: 2018/11/30-06:32:22-UTC, 2018/11/12-20:13:57-UTC,
2018/11/11-23:34:44-UTC

The recovery and alternate email addresses for GOOGLE ACCOUNT 1 are both ryanrocks462@yahoo.com (YAHOO ACCOUNT 1), and the associated phone number is 661-361-3779, which I recognize as the same phone number associated with HERNANDEZ's Yahoo (Oath) accounts.

101. According to Google IP logs, which were provided on about December 19, 2018, ryanrocks562@gmail.com (GOOGLE ACCOUNT 1) was accessed through HERNANDEZ HOME IP #1 and HERNANDEZ HOME IP #2 (172.248.227.193 and 76.232.194.142) of the **SUBJECT PREMISES**. For instance, below are login records provided by Google:

Time	IP Address	Type
2018/11/30-06:32:22-UTC	76.232.194.142	Login
2018/11/12-20:17:36-UTC	2606:6000:50cc:8000:195:6977:74e5:8fd2	Logout
2018/11/12-20:13:57-UTC	2606:6000:50cc:8000:195:6977:74e5:8fd2	Login
2018/11/11-23:34:44-UTC	2606:6000:50cc:8000:1c13:77e4:2563:e1de	Login
2018/10/21-20:37:55-UTC	172.248.227.193	Login
2018/07/14-10:59:57-UTC	172.248.227.193	Login

Moreover, I know that users of online accounts such as Google may, in fact often, remain logged into accounts for extended

periods of time. Here, the last action logged indicates a login on November 30, 2018, from HERNANDEZ HOME IP #2 (76.232.194.142) at the **SUBJECT PREMISES**, without a logout through the date of records production.

102. I also noted that the time period during which HERNANDEZ used HERNANDEZ HOME IP #1 and HERNANDEZ HOME IP #2 to access his various accounts corresponds with when HERNANDEZ is suspected of engaging in criminal activity over the Internet, also using HERNANDEZ HOME IP #1 and HERNANDEZ HOME IP #2.

103. For the reasons set forth in this affidavit, I believe that ample probable cause exists to conclude that the **SUBJECT PREMISES** contains evidence, instrumentalities and the fruits of the criminal activity described therein, which includes, among other things, various digital devices and the data stored thereon. Items seized will be transported to another district, including to the Western District of Washington where the investigation is being handled by the FBI Seattle Office. Further, the examination of computers and other digital devices will be conducted in a manner as set forth in Attachment B, which is incorporated herein.

TRAINING AND EXPERIENCE ON DIGITAL DEVICES¹⁸

104. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I

¹⁸ As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital

know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the

cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

105. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so

many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

106. The search warrant requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after

a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress HERNANDEZ's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of HERNANDEZ's face with his or her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

//

//

//

CONCLUSION

107. For all the reasons described above, there is probable cause to believe that the items listed in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 371 and 1349 (Conspiracy), 1028(a)(7) (Identity Theft); 1028A (Aggravated Identity Theft); 1029(a)(2) (Access Device Fraud); 1030(a)(2), (4) and (5)(A) (Computer Fraud/Hacking); and 1343 (Wire Fraud) will be found at the **SUBJECT PREMISES**, as described in Attachment A. Therefore, I respectfully request that this Court issue the requested search warrant for the **SUBJECT PREMISES**, more particularly described above and in Attachment A, authorizing the seizure of the items described above and in Attachment B.

/s/
Joel Martini, Special Agent
Federal Bureau of Investigation

Subscribed to and sworn before me
this 18th day of June, 2019.

MARIA A. AUDERO

HONORABLE
UNITED STATES MAGISTRATE JUDGE

NICOLA T. HANNA
United States Attorney
PATRICK R. FITZGERALD
Assistant United States Attorney
Chief, National Security Division
LISA E. FELDMAN (Cal. Bar No. 130019)
Assistant United States Attorney
Cyber & Intellectual Property Crimes Section
1500 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-0633
Facsimile: (213) 894-0141
E-mail: lisa.feldman@usdoj.gov

Attorneys for Applicant
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

IN THE MATTER OF THE SEARCH OF:

No. **2:19-MJ-02536**

40520 Aster Place, Palmdale,
California 93551

ORDER ALLOWING EXTENSION OF TIME
WITHIN WHICH TO RETAIN AND SEARCH
DIGITAL DEVICES

(UNDER SEAL)

For good cause shown, IT IS HEREBY ORDERED that the government may retain and search, pursuant to the terms of the original warrant in this matter, for an additional 120 days (beyond the time period previously authorized), to **February 13, 2020**, the following digital devices:

1. One (1) HGST hard drive, S/N: 130325TEA45A3R240BK;
2. One (1) HGST hard drive, S/N: 130301E20342BM0V340S;
3. One (1) Hitachi hard drive, S/N: 111223E20B12C7CGL9RS;
4. One (1) Toshiba hard drive w/ power cord, G003250A;
5. One (1) Nintendo Switch w/power cord, XAW10001300634;
6. One (1) Nintendo Switch w/power cord, XAL03100140300;
7. One (1) Seagate hard drive w/enclosure, S/N: Z84112WS,
S/N: NA8TLMT0;
8. One (1) Wii w/power cord, S/N: RMA200086644;
9. Two (2) 4GB Powersticks, Model PSPV1;
10. One (1) Apple Watch, FH7QM3CBGR7N;
11. One (1) adapter, E202650;

12. One (1) Motorola Micro SD adapter, 2010-06-12;
13. One (1) Kodak memory card 8GB w/case, 31295-8GBCSTA;
14. One (1) ETC hotels thumb drive, 1GB 1011S;
15. One (1) ETC hotels thumb drive, 1GB 1011S;
16. One (1) Casa del Mar ETC hotel flashdrive 2GB;
17. One (1) Transcend Micro SD adapter 32GB, 9181AA32G09QS2;
18. Four (4) CDs;
19. One (1) Nintendo 3DS w/adapter, EW100000054
20. One (1) Kingston Technologies hard drive 128GB,
50026B7726A02E6DE;
21. One (1) Nintendo WiiU, JW403398933;
22. One (1) IS-Nitro-Emulator, S/N: 08050639;
23. One (1) WiiU, FW705088709;
24. One (1) iPhone S, rose gold color, Model: A1633;
25. One (1) Nintendo Switch w/cradle and power cord,
XAW10021377616;
26. One (1) blue Nintendo 3DSXL, SW105787592;
27. One (1) iPhone, black, Model: A1778;
28. One (1) Nintendo WiiU black, FW99906933;
29. One (1) NDEV wireless w/power cord, S/N: NMA20089065;
30. One (1) WiiU, white w/controller S/N: FW090204951;
31. One (1) Macbook w/power cord, S/N: C02MN8TDFD57;
32. One (1) iPhone X, black, cracked back

October 15, 2019

DATE

Presented by:

/s/ [Lisa E. Feldman]
LISA E. FELDMAN
Assistant United States Attorney


UNITED STATES MAGISTRATE JUDGE
JEAN P. ROSENBLUTH